

# **ADVANCED CELL PHONE FORENSICS CONFERENCE**

February 8, 2019  
APAAC Training Room  
Phoenix, Arizona



## **CELLULAR ANALYSIS CONSIDERATIONS FOR CRIMINAL INVESTIGATIONS**

Presented by:

**Geoff Young**  
Special Agent

Distributed by:

ARIZONA PROSECUTING ATTORNEYS' ADVISORY COUNCIL  
1951 West Camelback Road, Suite 202  
Phoenix, Arizona 85015

ELIZABETH ORTIZ  
EXECUTIVE DIRECTOR



# **Cellular Analysis Considerations** **For Criminal Investigations**

**SA Geoffrey Young  
Cellular Analysis Survey Team  
Phoenix, AZ**

Cellular Analysis Survey Team Unit  
Violent Crimes Against Children Section  
Criminal Investigative Division  
Federal Bureau of Investigation



# Topics

1. CAST
2. Why cell phones?
3. Basics of Cellular Technology
4. Cell Site Analysis
5. Location Based Services
6. Cell Tracking (Cell Site Simulators)
7. Tower Dumps
8. Pre-paid (Drop) Phones
9. SMS Content
10. Network Survey Drive Testing



# 1. Cellular Analysis Survey Team

- 67 certified SA's and TFO's with a strong background in cell phone analysis, tracking, and understanding of the various cell phone technologies
- Received approximately 400 hours of specialized training
- Trained over 10,000 Federal agents, state investigators, as well as prosecutors, in the investigative technique.
- **Testify as expert witnesses in cell phone analysis**
  - Testified as expert witnesses in over 1,500 criminal trials.





# CAST Case Priorities

- Immediate Threats to Life
  - *Child Abductions*
- Terrorism
- Homicides and Kidnappings
- FBI Cases
- Other Agency Cases
- CAST will attempt to accommodate all cases
- Requests for assistance accepted at:
  - **CAST@ic.fbi.gov**



## 2. Why Cell Phones?

327 Million cell phones in use in the U.S.  
Only 317 Million people in the U.S. (per Wikipedia)

More than 6 Billion text messages are sent per day in  
the U.S. (per Forrester research)

- The prevalence of cell phones makes it likely that your Suspect and/or Victim carried a cell phone during the crime.
- The cell phone that your Suspect and/or Victim carries creates a wealth of evidence, such as location information, contact information, text/iMessage chats, internet search results, photographs, videos, apps.



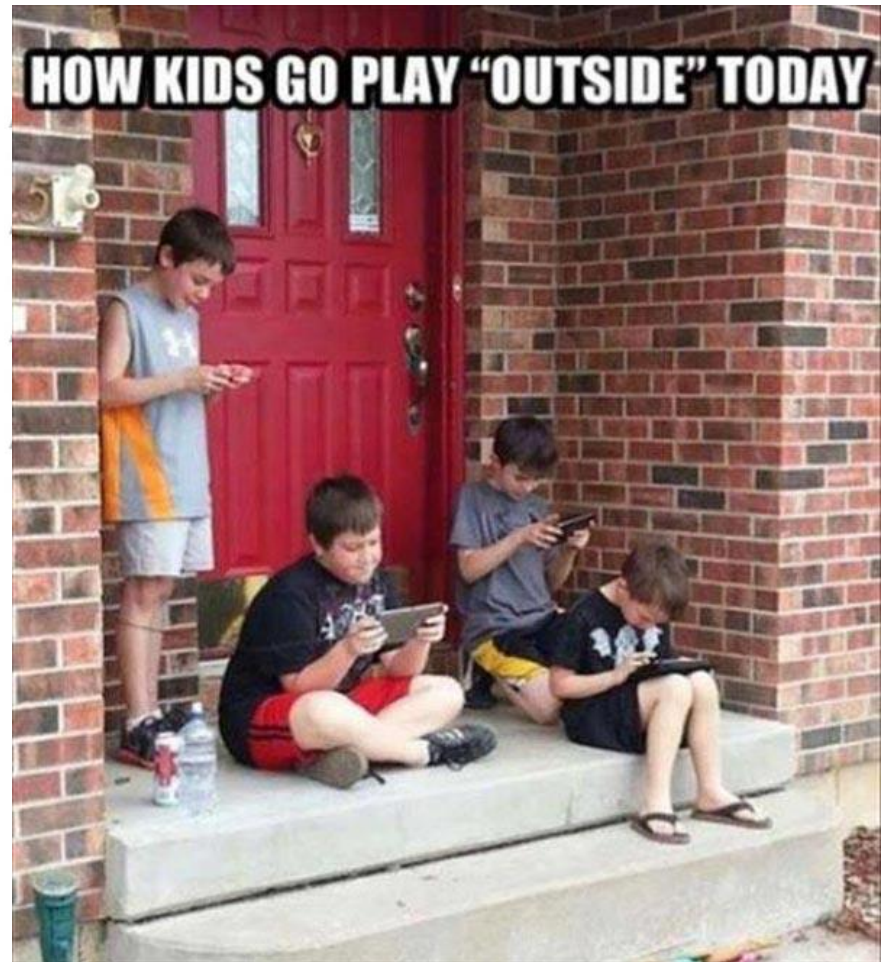
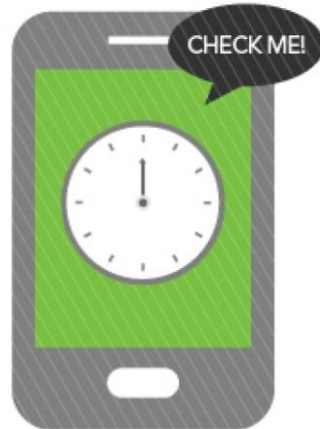
# Why Cell Phones?

WE'RE ADDICTED TO CHECKING OUR PHONES

**58%**

OF SMARTPHONE USERS

**DON'T GO  
1 HOUR  
WITHOUT CHECKING  
THEIR PHONES**



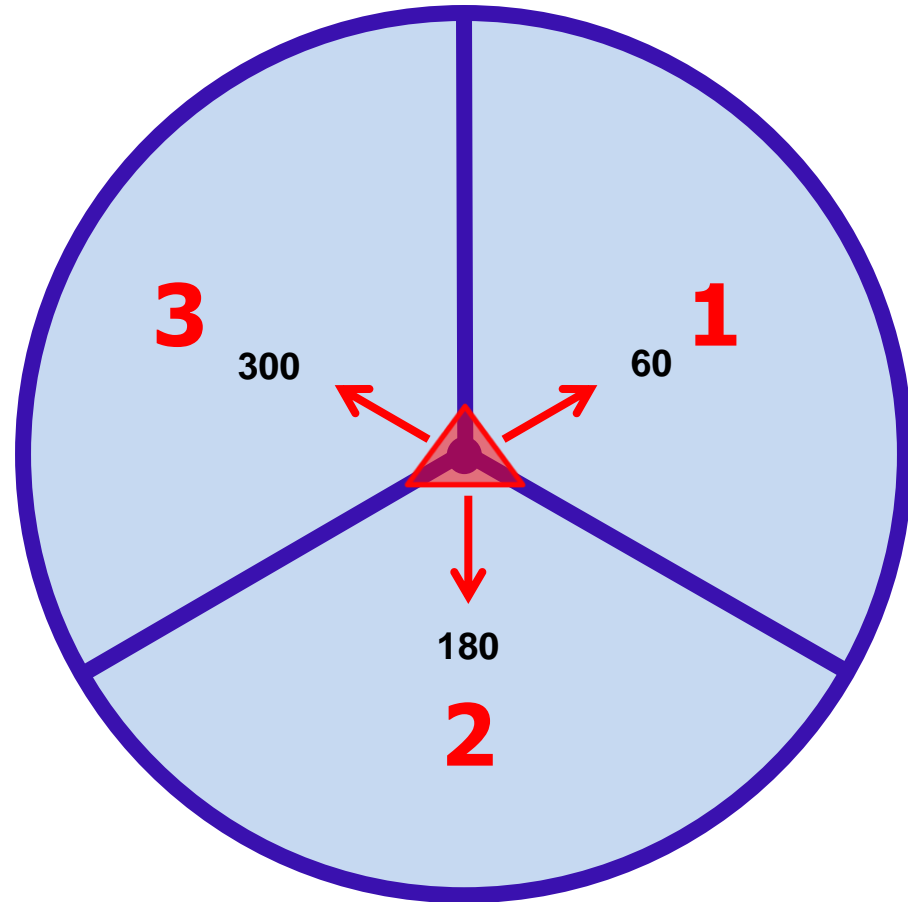
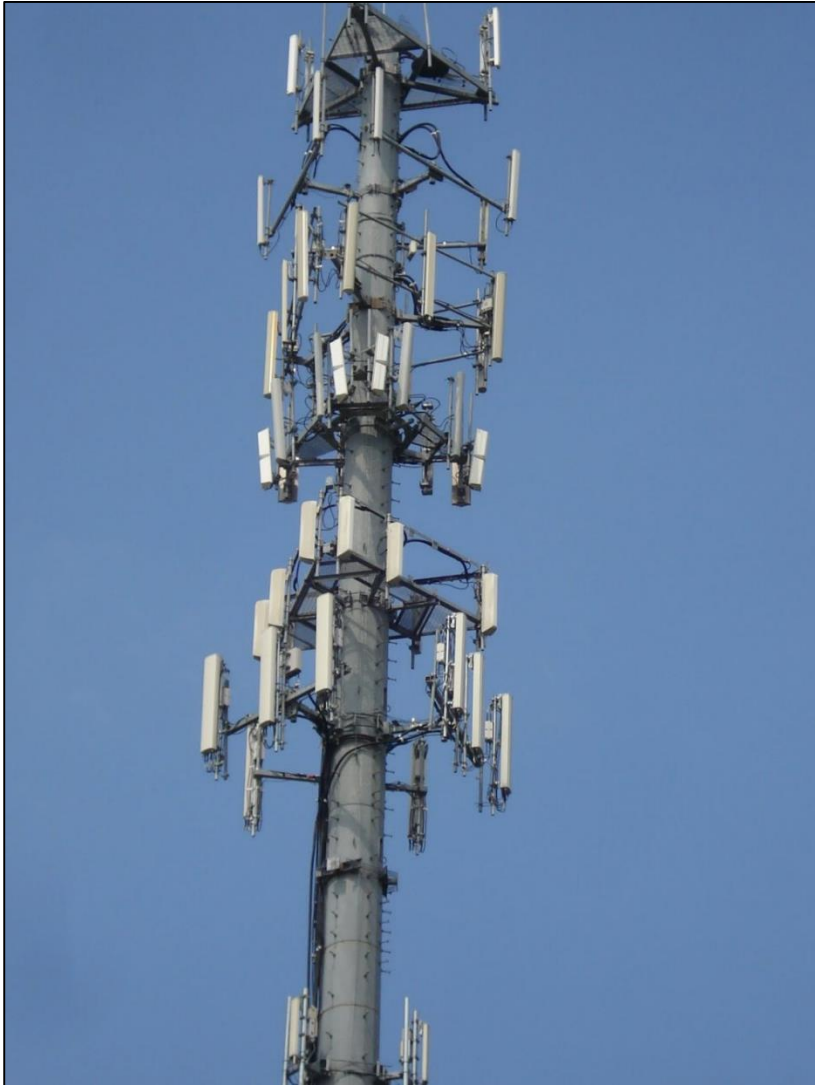


# 3. Basics of Cellular Technology





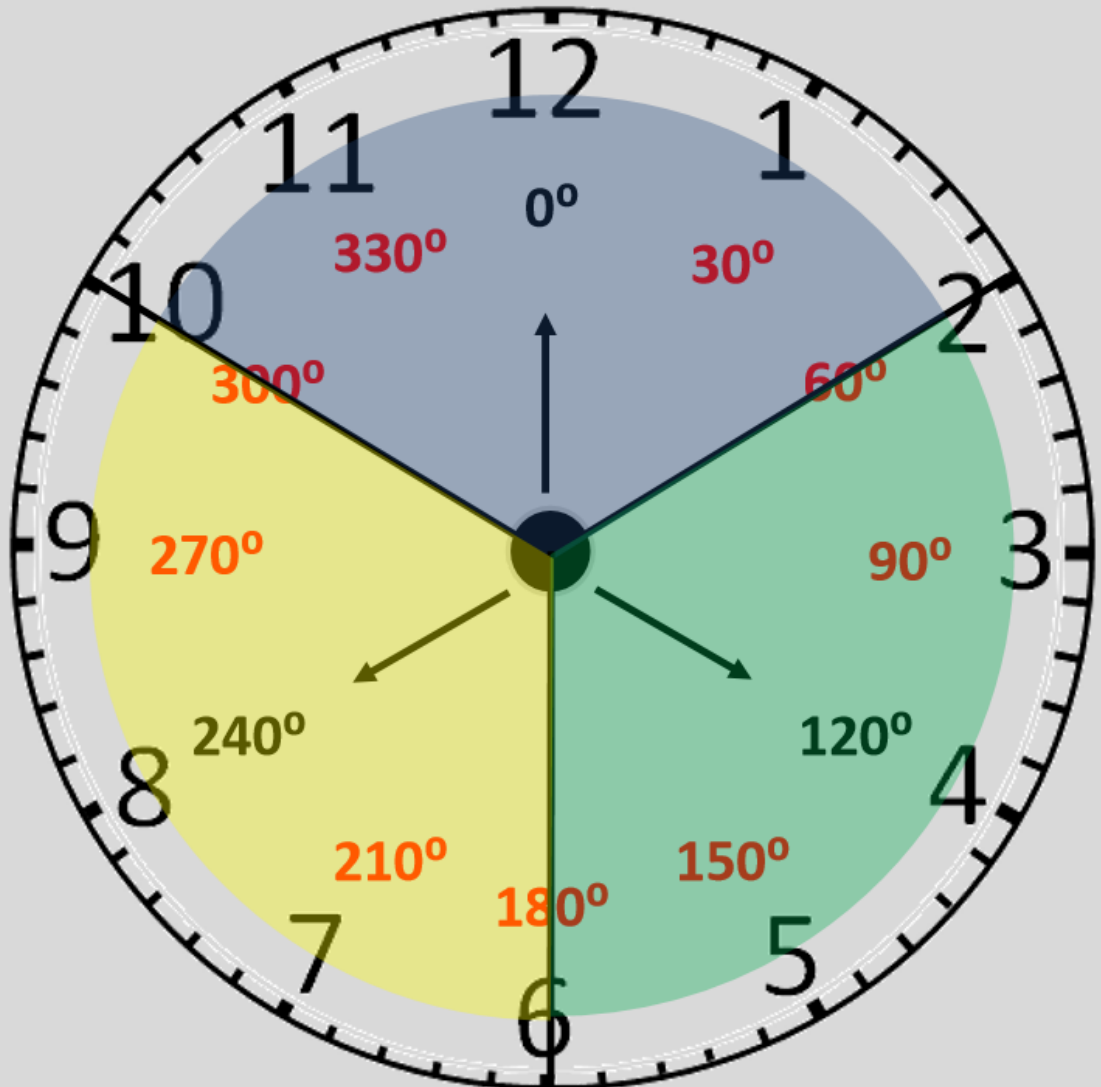
# Sectorization





# Understanding Azimuth

- Orientation (or direction) corresponds to times on a clock, with 12:00 o'clock being North
- Every hour on the clock is equal to 30 degrees
- If the orientation points at 0 degrees or 12:00 o'clock, the coverage can be approximated to be 60 degrees in either direction
- Likewise, for the remaining sectors





# Cell Site Location Information

Each cell sector has a unique Global Cell ID (GCI).  
Like a fingerprint, the GCI is unique on the network and is not duplicated.

(AT&T/T-Mobile) =  
Country Code + Network Code + Location Area Code + Cell Site ID

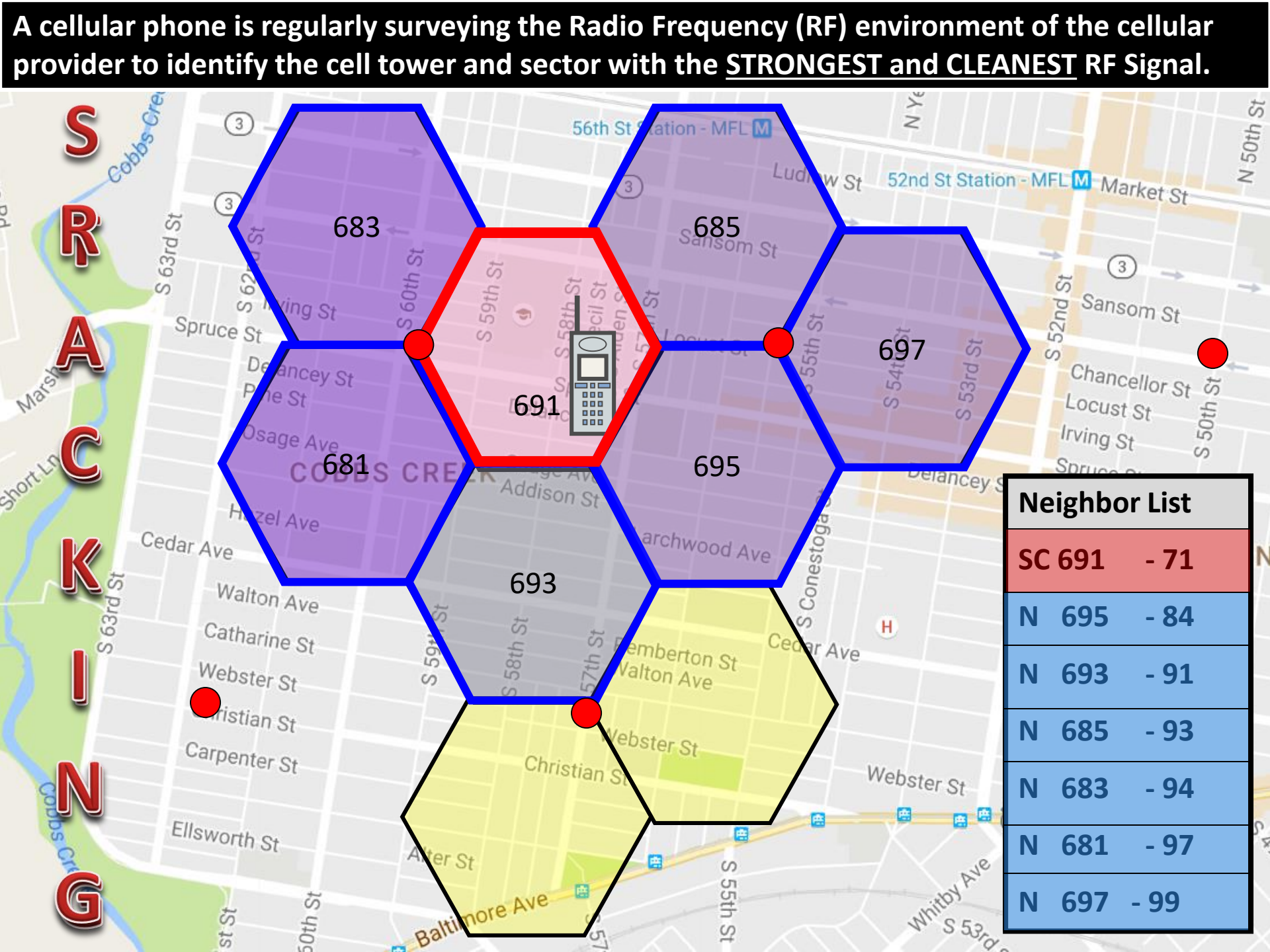
(Sprint/Verizon) =  
Country Code + Network Code + Switch/NEID+ Cell Site ID

We know where we are and what phone company we are working with  
so our focus is on the LAC + Cell Site ID (obtained from the records)

The network knows where the phone is and must keep track of the phone  
to some granularity in order for the network to provide necessary  
resources for call quality, network mobility and accurate billing.

A cellular phone is regularly surveying the Radio Frequency (RF) environment of the cellular provider to identify the cell tower and sector with the STRONGEST and CLEANEST RF Signal.

Neighbor List	
SC 691	- 71
N 695	- 84
N 693	- 91
N 685	- 93
N 683	- 94
N 681	- 97
N 697	- 99



Neighbor List		
SC 691	-	71
N 695	-	84
N 693	-	91
N 685	-	93
N 683	-	94
N 681	-	97
N 697	-	99



# CDRs and Tower Lists

**CDR**

	Date	Time		LAC/Switch	Sector	Tower
	10/30/2012	9:10 AM		PHX	1	123

**TOWERS**

LAC/Switch	Tower	Sector	Latitude	Longitude		Azimuth
PHX	123	1	43.156451	-89.287991		120



# CDRs and Tower Lists

**CDR**

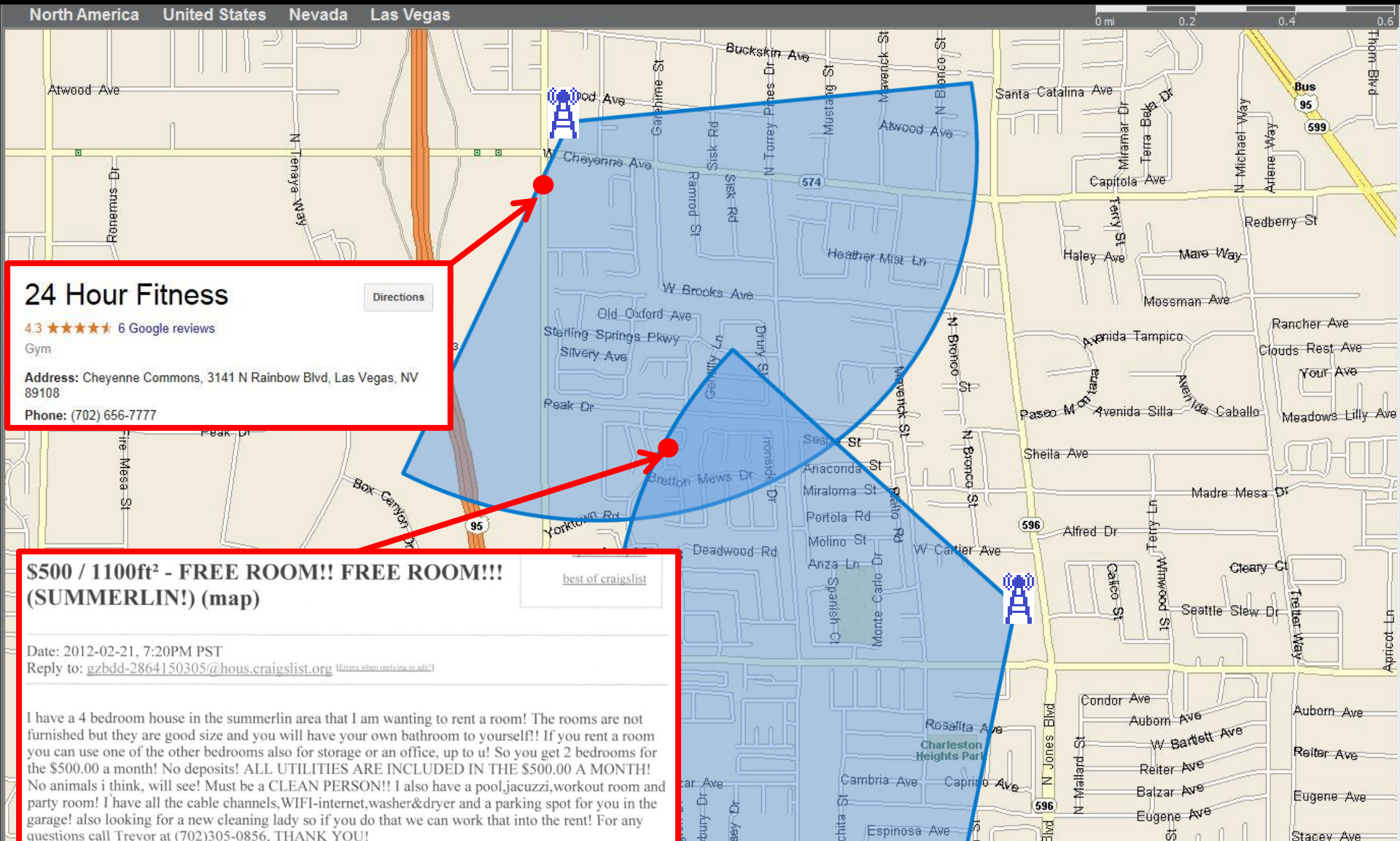
	Date	Time		LAC/Switch	Sector	Tower
	10/30/2012	9:10 AM		PHX	1	123

**TOWERS**

LAC/Switch	Tower	Sector	Latitude	Longitude		Azimuth
PHX	123	1	43.156451	-89.287991		120



# Mapping Cell Tower Activations (closed sector shapes - the old way)



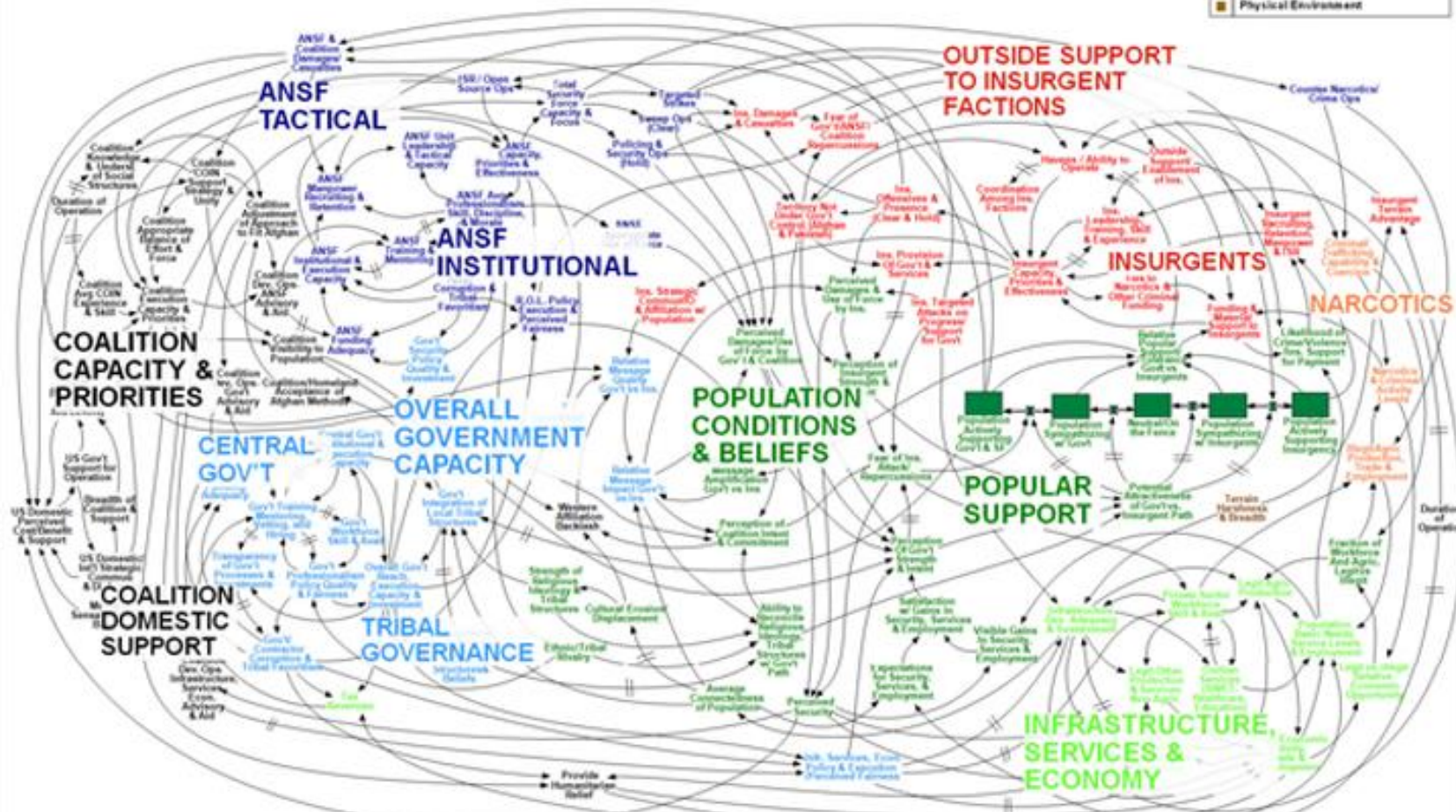
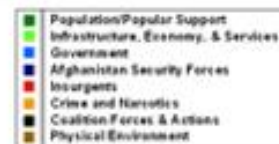


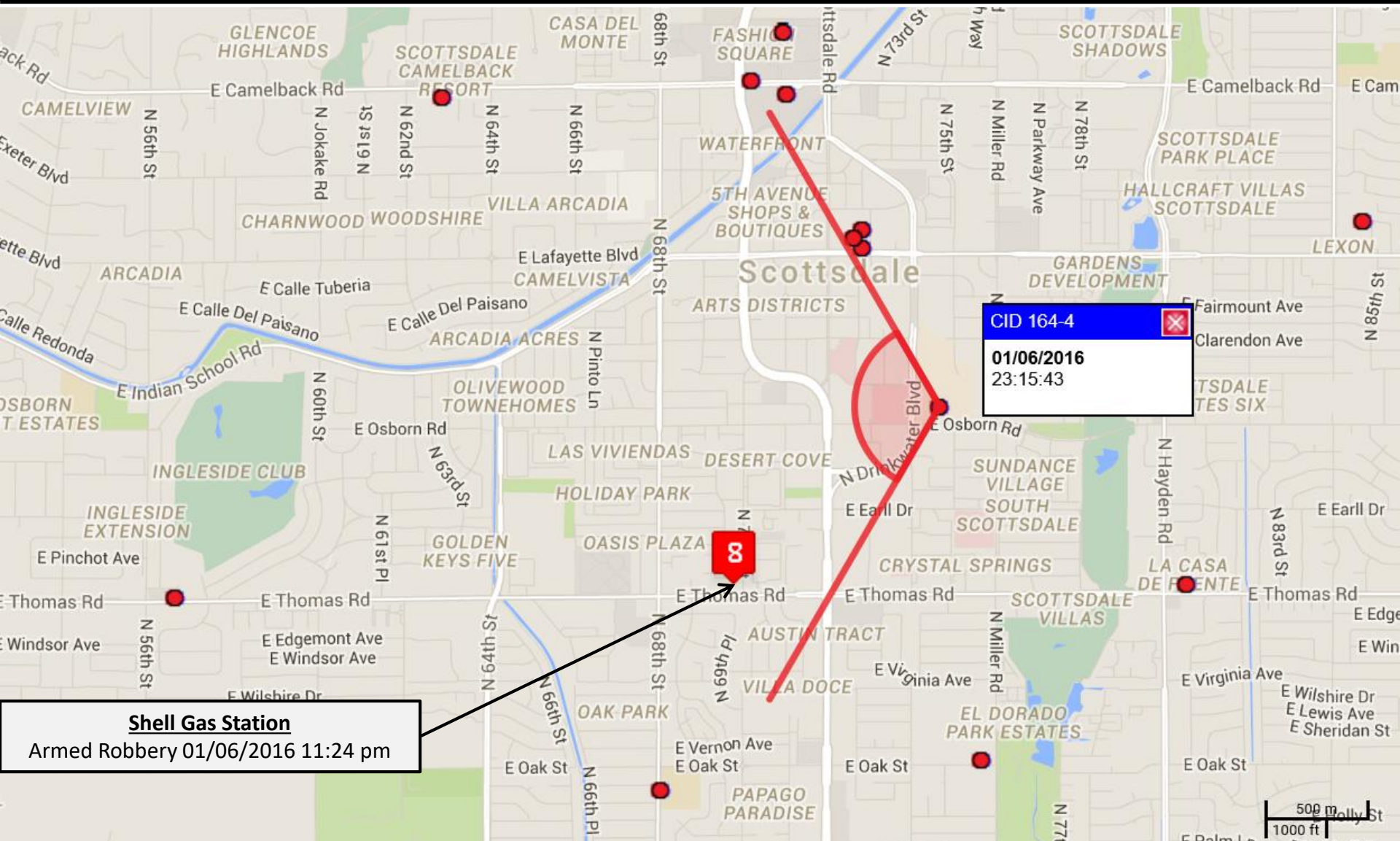
# Using Cell Site Analysis at Trial?

## KISS – Keep It Simple

### Afghanistan Stability / COIN Dynamics

// = Significant Delay

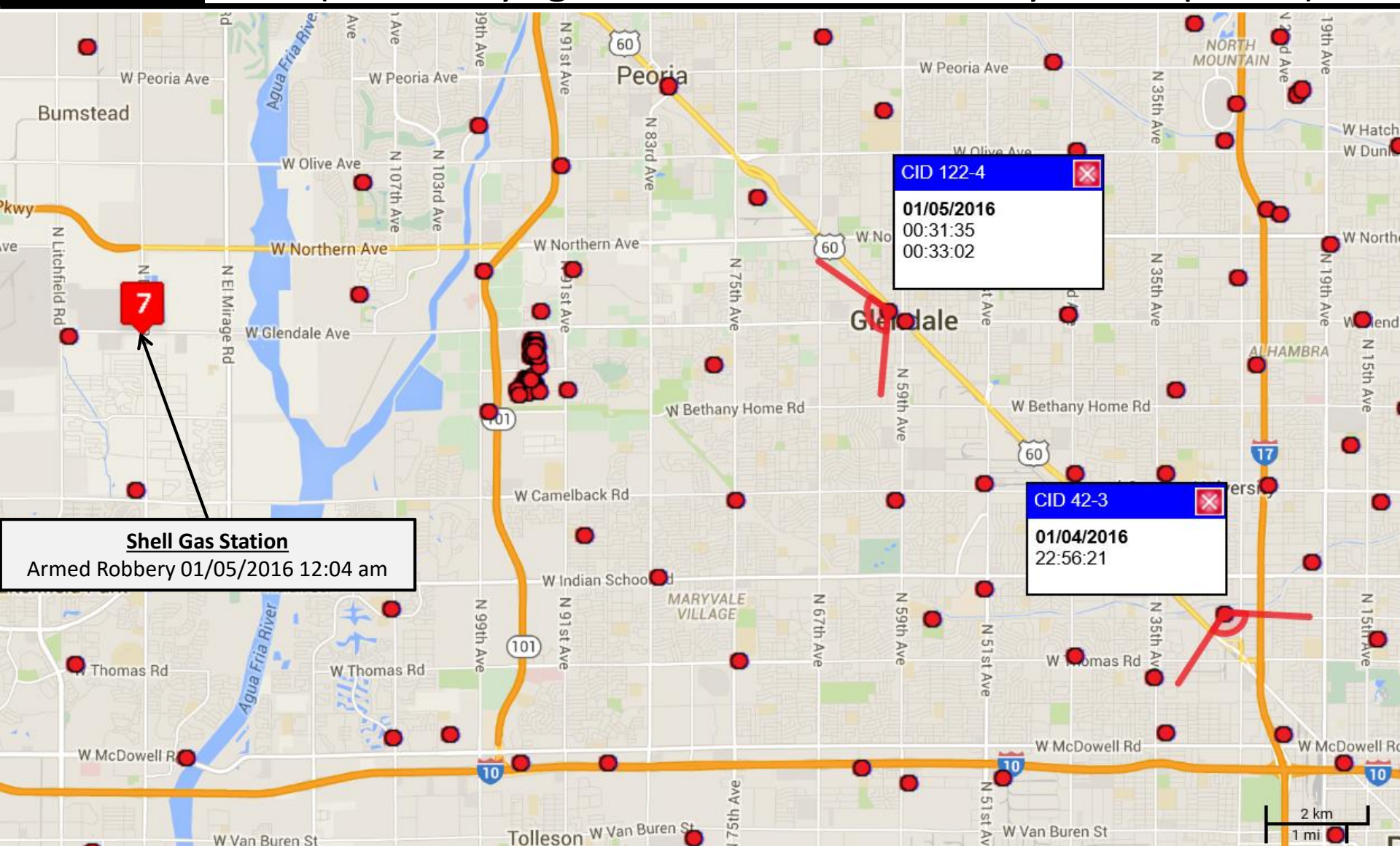






# Historical Cell Site Analysis

(Not always good evidence - limited by use of phone)





## 4. Cell Site Analysis

- “An analysis of Call Detail Records (CDRs) to determine where the cell phone was, where it is, or where it will be.”
  - Identifying information about a suspect, accomplices, associates and witnesses
  - Establish normal patterns (where the suspect works, stays at night, hangs out)
  - Corroborate or refute an alibi
  - **Determine location of a phone relative to a crime scene**
  - Along with other facts, could establish that target cell phone is in Suspect’s hands



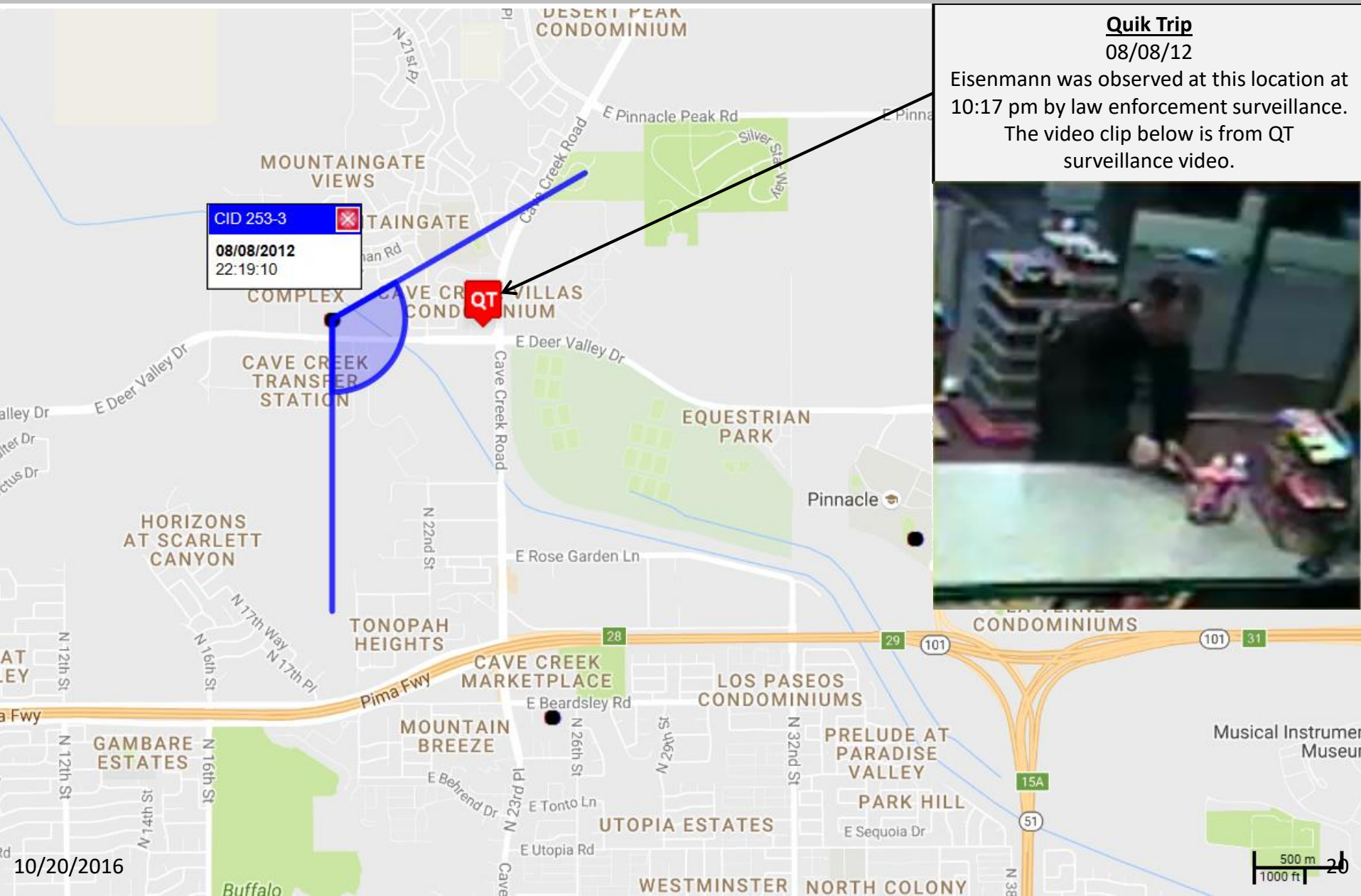
# Some Ways to Establish Possession

- Subscriber information from provider
- Call detail and frequency analysis
- Pattern of life analysis (home, work, frequent sector, last/first sector)
- Store video of purchase of phone
- Other video combined with cell site analysis (EXAMPLE TO FOLLOW)
- Social media!
- DES, utilities, credit reports, police reports and FI cards
- Address book/contacts from other phones
- SMS content
- Physical possession of the phone upon arrest, search, etc
- Interviews with associates, family, friends
- “Who was using the cell phone at the time is a question for the jury”

# GARY EISENMANN 602-425-0090 Historical Cell Site Analysis

08/08/2012 10:19 pm

Note: The call on [602-425-0090](tel:602-425-0090) at 10:19:10 pm was an incoming call.





# Determine Service Provider

Fone Finder

[www.fonefinder.net](http://www.fonefinder.net)

Reverse Phone Directory

[www.reversephonedirectory.com](http://www.reversephonedirectory.com)



Locate Plus

[www.Ippolice.com](http://www.Ippolice.com)



CLEAR

[www.cpclear.com](http://www.cpclear.com)



TARGUS

[www.targusinfo.com](http://www.targusinfo.com)

FBI ACS (internal FBI only)

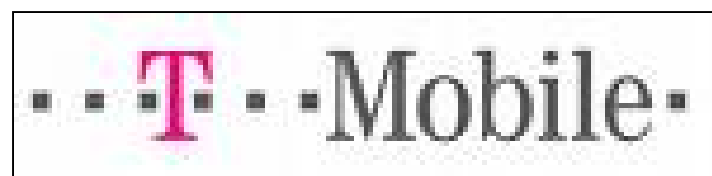


*Indicates paid subscription required*

**Bottom line: Call who you believe is the service provider to confirm it is their number!**



# Cellular Providers





# MVNO (Cellular Reseller)

- Mobile Virtual Network Operator
- MVNO's re-sell time on existing physical networks, focusing on specialized customer service and calling plans. They are fully dependant on the physical network for quality and coverage.
- Examples: Boost (Nextel), Virgin (Sprint), NET10 (AT&T), Tracfone (AT&T and T-Mobile)
- Subscriber and toll info kept by MVNO, call detail records (including cell site) kept by owner of network (same for roaming phones)



# Steps for Success

- Conduct exigent request, or obtain proper legal paperwork (court order or search warrant)
- Request call detail records for voice, SMS, and data sessions with **cell site** (cell tower) AND **cell sector** information
- Location Based Services (RTT, PCMD, GPS, etc.)
- Content when available (pending SMS, Voicemail, etc) – company dependent
- Tower listings for the time of the crime.
- Obtain digital records (Excel or text file format)



# Legal Standards

- Subscriber info - subpoena or higher
- Call Detail Records (CDR's) - subpoena or higher
- CDR's with cell site location information - search warrant (post SCOTUS Carpenter v. United States decision)
- RTT/PCMD data - search warrant
- Pen/Trap - 3123 court order or search warrant
- Cell Site Simulator (CSS) - search warrant
- Tower Dump Records - court order
- SMS content - search warrant or exigency
- Voicemail content - search warrant or exigency



# 5. Location Based Services

## Provider Contacts and Location Based Services Info

Sprint	T-Mobile	AT&T	Verizon
<p><b>(800) 877-7330</b> Fax (816) 600-3100</p> <p><b>L- Site “Ping”</b></p> <p><b>GPS coordinate of phone and suspected radius</b></p> <p><b>Set up through L-Site</b></p> <p><b>Pings can occur every 15 mins for 30 days</b></p> <p><b>Only provider that offers a web interface and is user friendly</b></p> <p><b>PCMD historical data</b></p>	<p><b>(973) 292-8911</b> Fax (973) 292-8697</p> <p><b>E-911</b></p> <p><b>Triangulation of phone and suspected radius</b></p> <p><b>Results e-mailed to whatever address you want</b></p> <p><b>Results provided every 15 mins for 30 days</b></p> <p><b>True Call timing advance report with cell site, sector, and distance from tower</b></p>	<p><b>(800) 635-6840</b> Fax (888) 938-4715</p> <p><b>AT&amp;T Mobility Locator</b></p> <p><b>GPS coordinate of phone and suspected radius</b></p> <p><b>Results emailed to whatever address you want</b></p> <p><b>Results provided every 15 mins for 30 days</b></p> <p><b>NELOS report contains historical locations</b></p>	<p><b>(800) 451-5242</b> Fax (800) 345-6720</p> <p><b>Real Time Tool (RTT)</b></p> <p><b>NOT a true real time measurement tool</b></p> <p><b>Is based ONLY on LAST call/txt/data activity, cannot ping the phone</b></p> <p><b>Provides cell site and sector, and possible distance from tower</b></p> <p><b>Must call each time to get results</b></p> <p><b>Verizon will suggest that you get a PR/TT</b></p>



UNCLASSIFIED//LES

# Provider Retention Periods

(As of 8/10/2017)

Provider	AT&T	Cricket (AT&T)	T-Mobile	MetroPCS (T-mobile)	Sprint	Verizon	US Cellular
Subscriber	7/14/2008 to present	~6 months (ending April 2016)	2002 to present	180 days	18 months	3-5 years	~7 years
Call Detail Records	7/14/2008 to present	~6 months (ending April 2016)	2002-present (postpaid); 2 years rolling (prepaid)	180 days	18 months; backup tapes available 2005 to present	1 rolling year	1 rolling year
Cell Site (Voice)	7/14/2008 to present	~6 months	90 days (moving to 2 years); (mediation = 10/2013 to present)	6 months	18 months	1 rolling year	1 rolling year
SMS tolls	2/11/2010 to present	6 months	2002-present (postpaid); 2 years rolling (prepaid)	180 days	18-24 months	1 year	1 rolling year
Cell Site (SMS)	~1 year	No	90 days (moving to 2 years); (mediation = 10/2013 to present)	No	No CDR, Yes Reveal (PCMD)	No CDR, Yes RTT (PCMD)	No
SMS content	No (AT&T msg app 90 days; ~10%)	No	No	60 days (CDMA only)	Only on T-III	3-10 days max.	3-5 days
Cell Site (Data)	4/9/2010 to present	No	No	No	18 months (if request IPDR Report)	1 rolling year (orig tower only)	No
Tower Dumps	7 years	6 months	180 days	6 months	18 months	1 year	1 year
Prospective	Mobile Locate (Triangulation / AGPS)	No	E911 (Triangulation)	No	GPS "Ping" (device dependent)	No (see RTT)	No, but force "no ring" call
PCMD/RTT (Historic)	No, but NELOS (~13 months)	No	No	No	PCMD (~90 days voice; 2 weeks SMS/data)	RTT (7-8 days)	PCMD (14-29 days)
WiFi Calling	Pending	No	App / Open WiFi	Yes (no location info)	App / Open WiFi	Pending	No
VoLTE	No	No			No	16 devices [orig tower only]	
Store Video			30 days (sbp)		2-3 months (sbp)	30-90 days (sbp)	
Voicemail			yes			No	
Cloud Storage	Via Synchronoss					Via Synchronoss	
Internet/Web Browsing	Rolling 13 months				If we have to go to tapes, it's a 6 month turnaround	"IP Sources Destination" 180 days	



# Phrases to Use for Historical Records Court Orders

- AT&T - “All Available records to include call detail, SMS, data, **NELOS**, and cell site and cell site sector information from (date) to present”
- Sprint - “All Available toll records to include call detail, SMS detail, data sessions, **per call measurement data (PCMD)**, cell site and cell site sector information from (date) to present”
- T-Mobile - “Such service provider shall initiate a signal to determine the location of the subject’s mobile device on the service provider’s network or with such other reference points as may be reasonable available and at such intervals and times as directed by the law enforcement agent serving this order” \* **You must use this language for T-Mobile E-911 locator**
- Verizon - “All Available toll records to include call detail, SMS detail, data session, **Real Time Tool (RTT) data**, cell site and cell site sector information from (date) to present”
- **I have an updated sample language document I can e-mail.**



# Real-Time Location Based Services

GMLC.AT&T.Mobility.Compliance@bspfnc01.edc.cingular.n

5:36 AM (11 hours ago) ☆



to ▾

AT&T PROPRIETARY Solely for authorized persons having a need-to-know pursuant to Company instructions

AT&T CONFIDENTIAL - DO NOT FORWARD.

Initiated 2013/08/28 05:35:50 Pacific

The mobile number was located on 8/28/2013 12:36:6 GMT

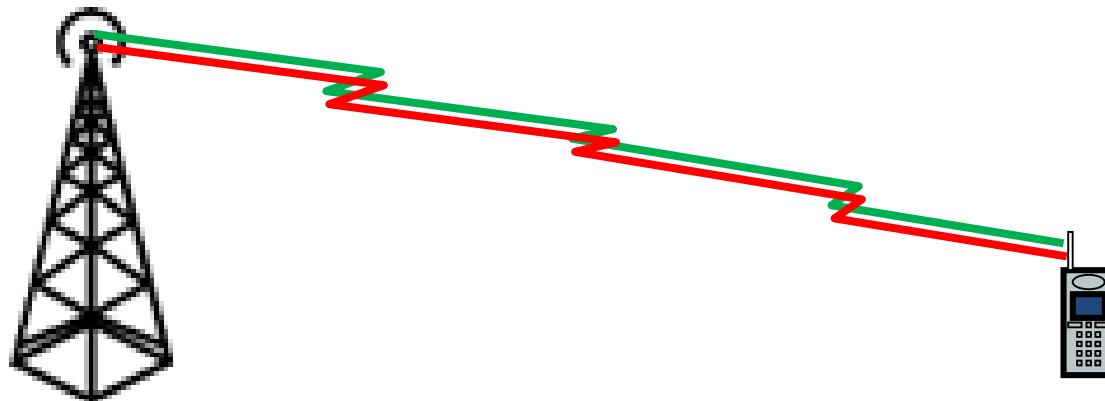
ITN	1392202
Case ID	XXXXXXXXXXA170
Mobile Number	XXXXXX6285
Confidence Level	&nbsp;
Longitude	066 51 17.512W
Latitude	18 01 35.551N
Radius	14 meter (Certainty Factor)
Data Source	3G-GMLC

**Do NOT  
send SWAT  
to hit the  
house!**



# Per Call Measurement Data (PCMD)

- PCMD is a method used by several CDMA supported cellular carriers to capture the approximate distance of a cellular phone from the tower.
- PCMD uses Round-trip time (RTT), also called round-trip delay (RTD), the time required for a signal pulse or packet to travel from a specific source to a specific destination and back again.
- In this situation, the source is the tower antenna initiating the signal and the destination is a cellular phone that receives the signal and responds back to the tower antenna.







# Real Time Tool (RTT)

- Sprint's PCMD data is called PCMD, but...
- Verizon's PCMD data is called Real Time Tool (RTT). The determined distance from the tower to the device is called the Access Distance and is displayed in the RTT report.
- The access distance arc is the calculated estimated distance the cellular device was from the tower.
- The RTT access distance is plotted with a margin of error arc applied before and after the access distance.
- The RTT access distance is plotted with a margin of error arc applied before and after the access distance.
- When additional RTT data is provided indicating a different utilized tower and sector with a band that overlaps the initial arc, that overlap area can become a higher probability region for the cellular device location.



# Historical Location Based Services

		CALL START TIME	CELL ID	SECTOR	DISTANCE (In Miles)	LATITUDE	LONGITUDE
		4/08/15 10:32:58	4	2	0.58	33.36716373	-112.2518311
							

		CALL START TIME	CELL NUMBER	SECTOR	RTD	LATITUDE	LONGITUDE
		4/08/15 10:32:58	4	2	0.58	33.36716373	-112.2518311
							



# *PCMD/RTT* Case Example

Cell Site Activations / RTT  
05/31/2018 3:53 PM

602-402-9371

SP

Crime Scene – Steven Pitt killed 05/31/2018 5:23 PM  
15849 North 71st Street, Phoenix, AZ

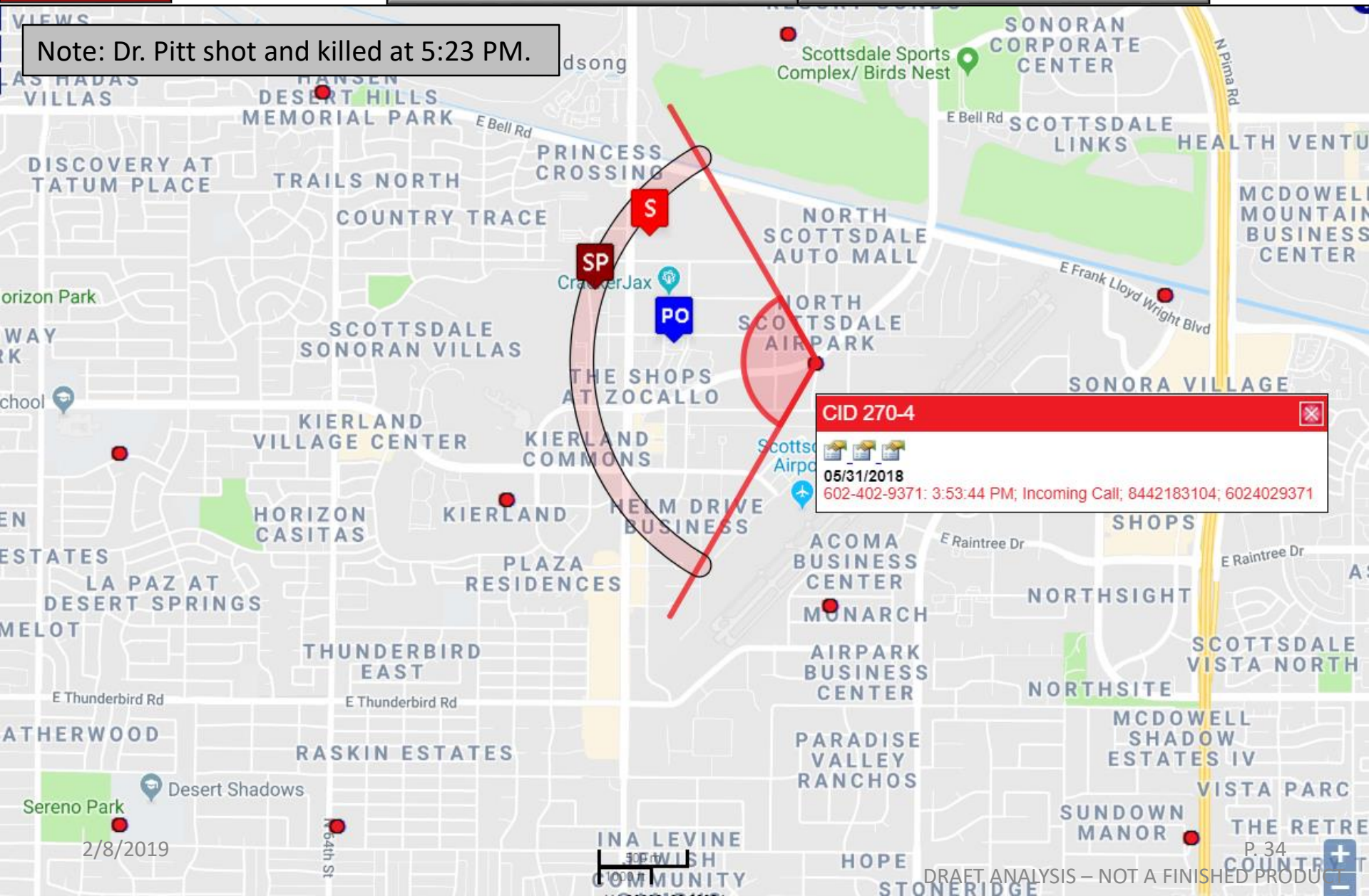
S

Subscriber Address for x9371  
16211 N. Scottsdale Rd, Scottsdale, AZ

PO

PO Box Jones used circa 2009  
15501 N. Scottsdale Rd, Scottsdale, AZ

Note: Dr. Pitt shot and killed at 5:23 PM.



2/8/2019

P. 34

DRAFT ANALYSIS – NOT A FINISHED PRODUCT

602-402-9371

CID 42-3



06/02/2018

602-402-9371: 2:03:37 PM; Outgoing Call; 6024029371; 86  
602-402-9371: 2:07:52 PM; Incoming Call; 6022993777; 6024029371  
602-402-9371: 3:13:34 PM; Outgoing Call; 6024029371; 674805980967  
602-402-9371: 3:19:06 PM; Outgoing Call; 6024029371; 674804421117  
602-402-9371: 3:34:05 PM; Outgoing Call; 6024029371; 674805858272

Note: Jones placed an outgoing call at 3:34:05 PM to victim Mary Simmons' number (x8272), blocking his number by dialing \*67 first.

CID 43-2



06/02/2018

602-402-9371: 2:07:00 PM; Outgoing Call; 6024029371; 6022993777

2/8/2019

500 m  
1000 ft

Cell Site Activations / RTT  
06/03/2018 11:30 AM -1:34 PM

MS

Crime Scene – Simmons/Thomas Homicides 06/03/2018  
14906 E. Kit Fox Pl, Fountain Hills, AZ

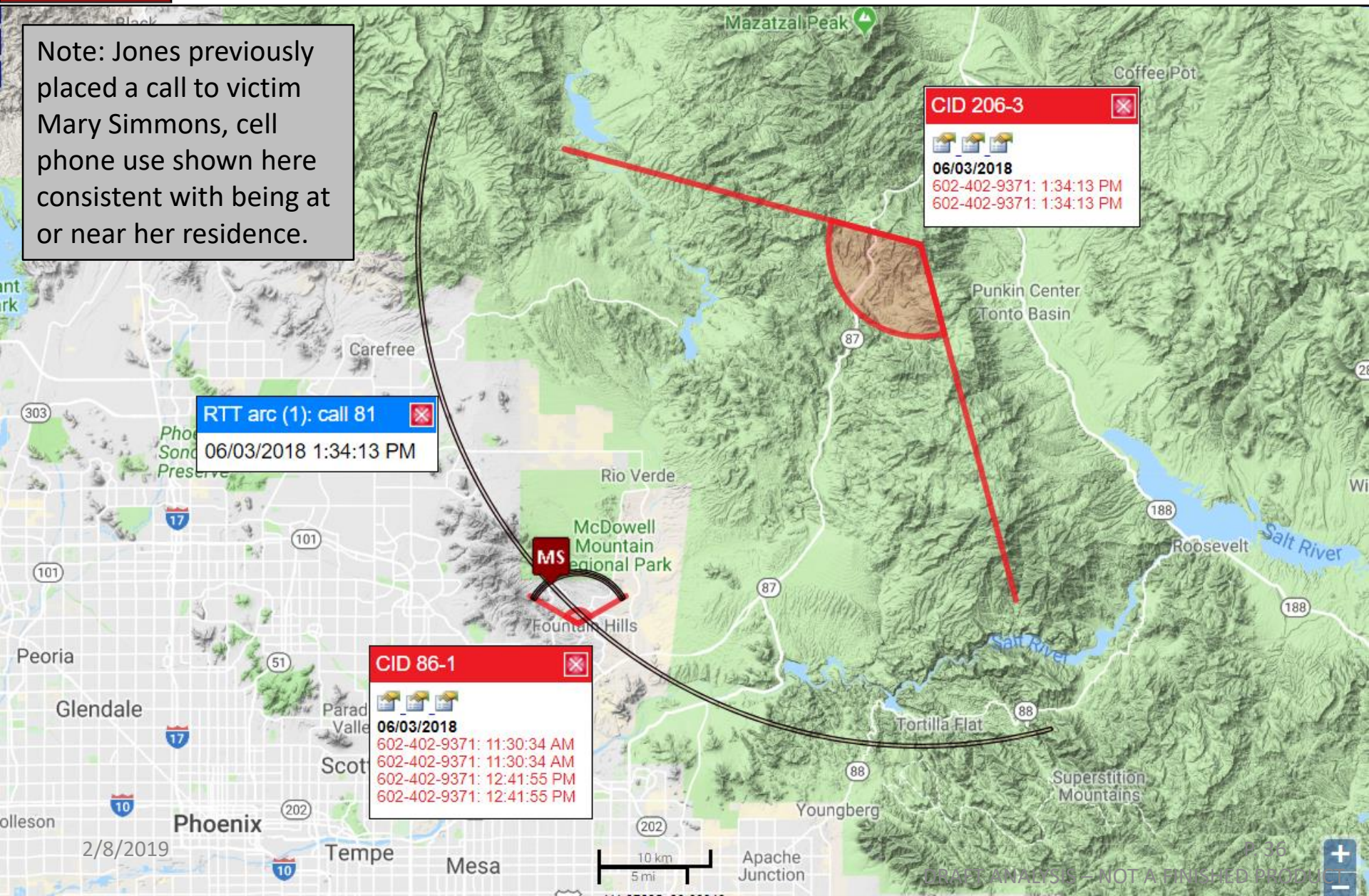
602-402-9371

Note: Jones previously placed a call to victim Mary Simmons, cell phone use shown here consistent with being at or near her residence.

RTT arc (1): call 81  
06/03/2018 1:34:13 PM

CID 206-3  
06/03/2018  
602-402-9371: 1:34:13 PM  
602-402-9371: 1:34:13 PM

CID 86-1  
06/03/2018  
602-402-9371: 11:30:34 AM  
602-402-9371: 11:30:34 AM  
602-402-9371: 12:41:55 PM  
602-402-9371: 12:41:55 PM

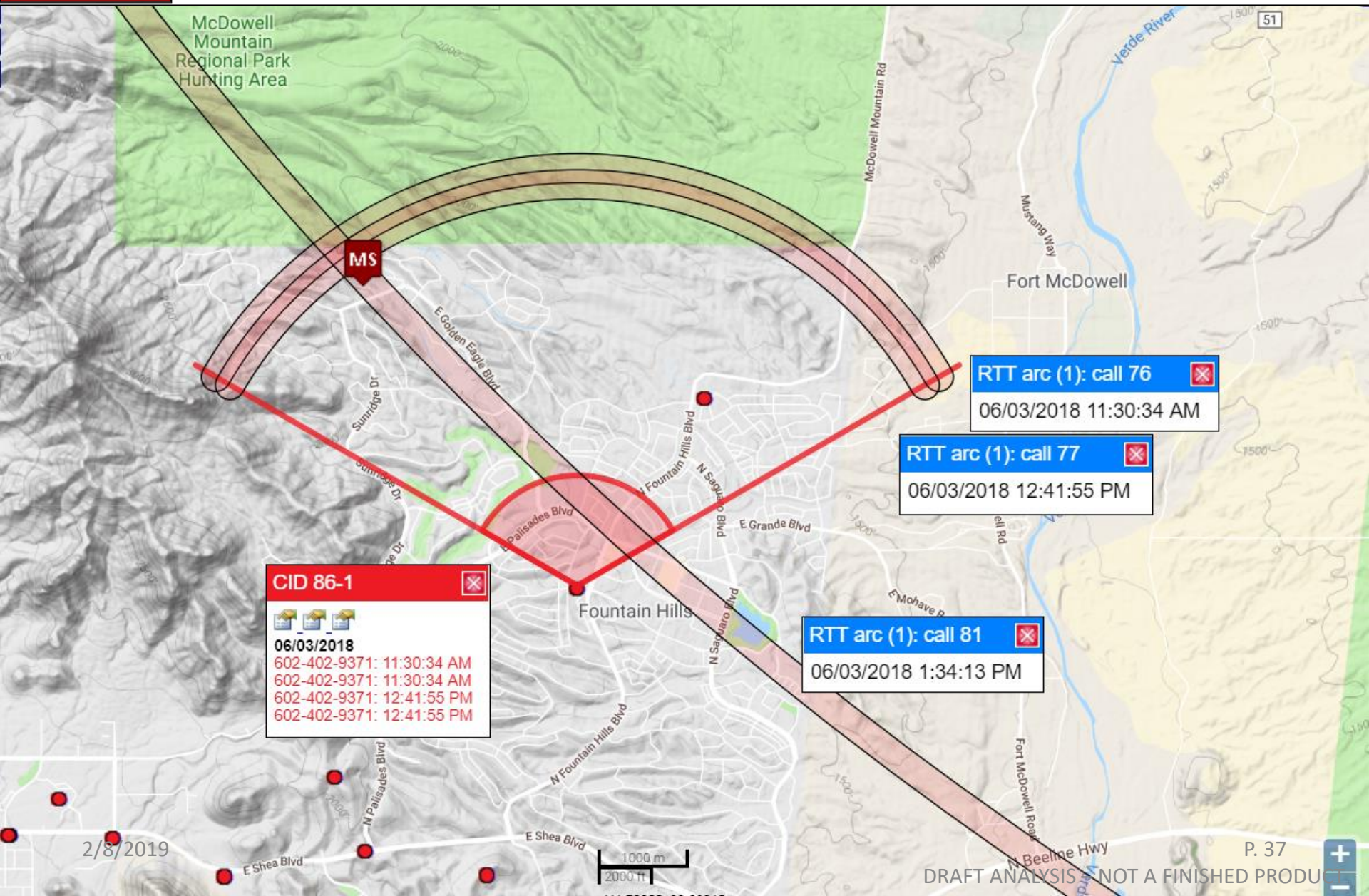


Cell Site Activations / RTT  
06/03/2018 11:30 AM -1:34 PM

MS

Crime Scene – Simmons/Thomas Homicides 06/03/2018  
14906 E. Kit Fox Pl, Fountain Hills, AZ

602-402-9371





# Other Considerations

- Google Location information
  - Google location info based on GPS, wifi, and cellular
  - Identify the Google account - can be associated with any email address, not just Gmail
  - Can request via exigent circumstances
- Apple may also have location information, but identified by the Apple ID
  - Keep in mind Apple phones can log into Google accounts (i.e. Gmail), and use Google apps



# Google Location Information Case Example

Note: This graphic intended to show general movement of cell phone in direction of arrow shown.

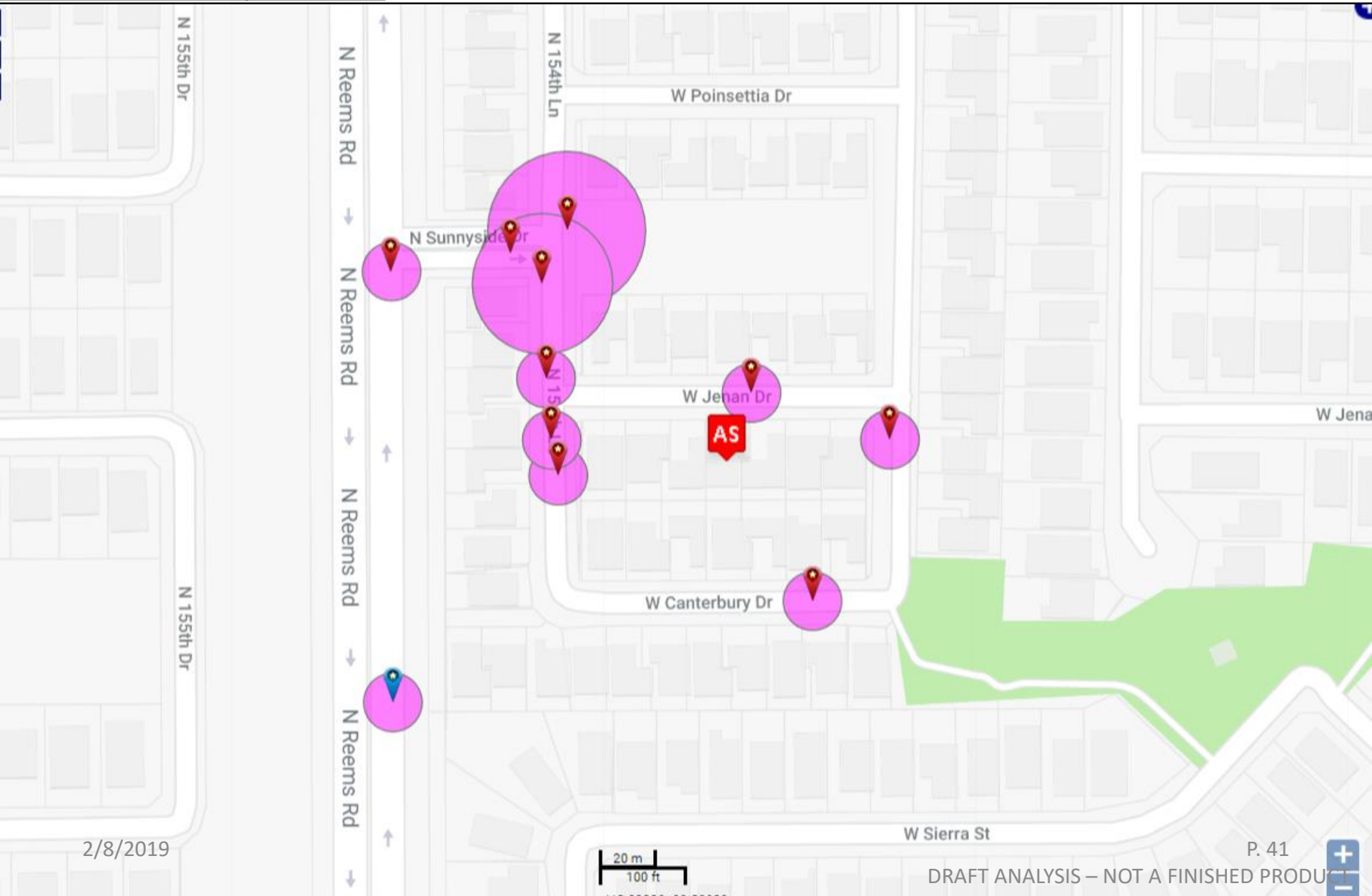
Geo-loc: 2334860  
9/9/2018 3:51:24 PM : 267-471-7133 ;  
35.977742 ; -115.156895 ; R10

Geo-loc: 2335451  
9/8/2018 4:26:37 AM : 267-471-7133 ;  
33.591212 ; -112.39234 ; R10

Geo-loc: 2340703  
9/6/2018 7:00:48 PM : 267-471-7133 ;  
29.708392 ; -96.504711 ; R10

Google 1

Google 2



2/8/2019

20 m  
100 ft

W Sierra St

P. 41

DRAFT ANALYSIS – NOT A FINISHED PRODUCT

Google 1

Google 2



Geo-loc: 2335451

9/8/2018 4:26:37 AM : 267-471-7133 ;  
33.591212 ; -112.39234 ; R10



Abduction Site  
15xxx W. Jenan Dr, Surprise, AZ



Quality Inn  
11201 Grand Ave, Youngtown, AZ

Google 1

Google 2

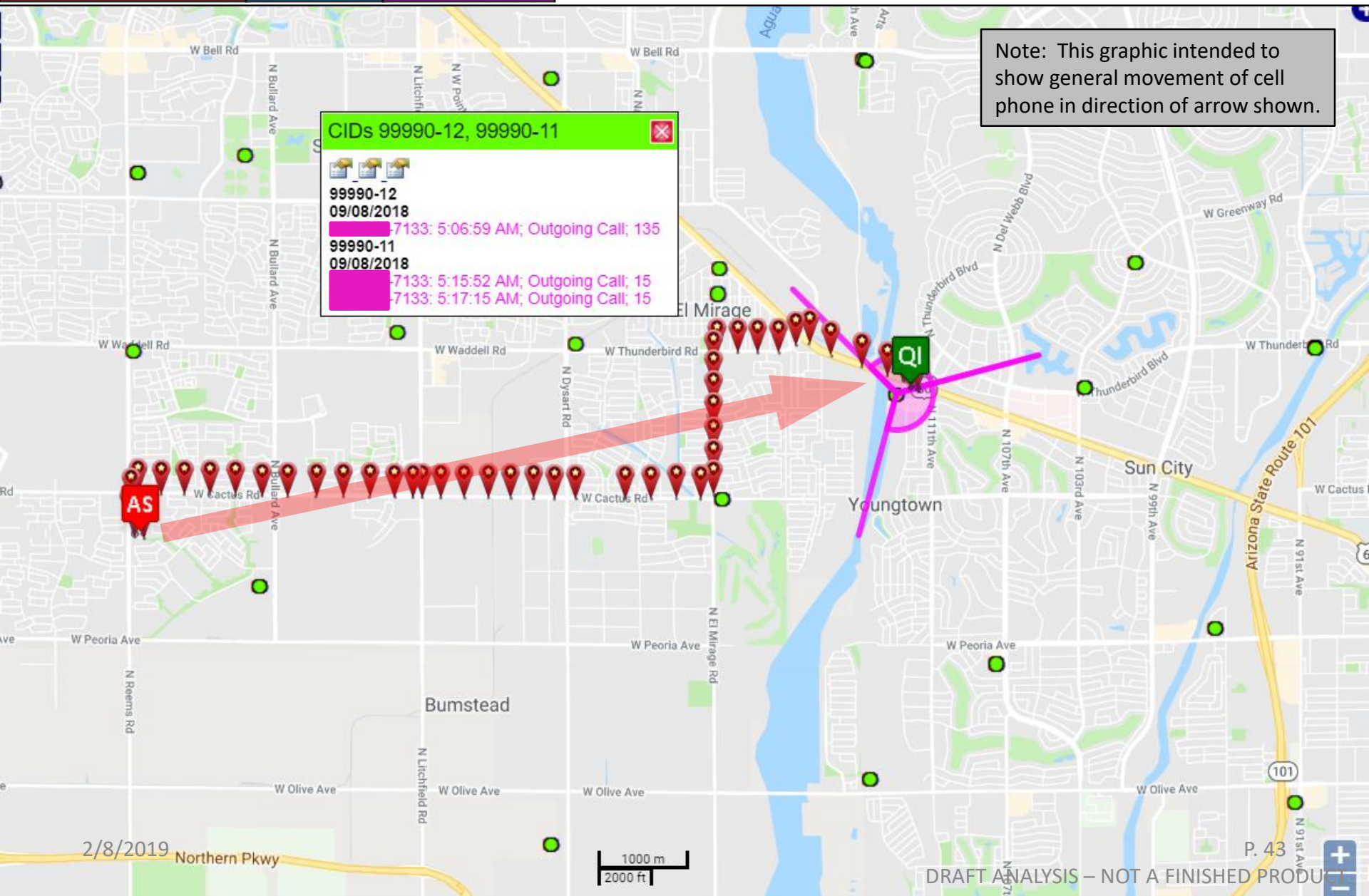
XXX-XXX-7133

Note: This graphic intended to show general movement of cell phone in direction of arrow shown.

CIDs 99990-12, 99990-11

99990-12  
09/08/2018  
7133: 5:06:59 AM; Outgoing Call; 135

99990-11  
09/08/2018  
7133: 5:15:52 AM; Outgoing Call; 15  
7133: 5:17:15 AM; Outgoing Call; 15





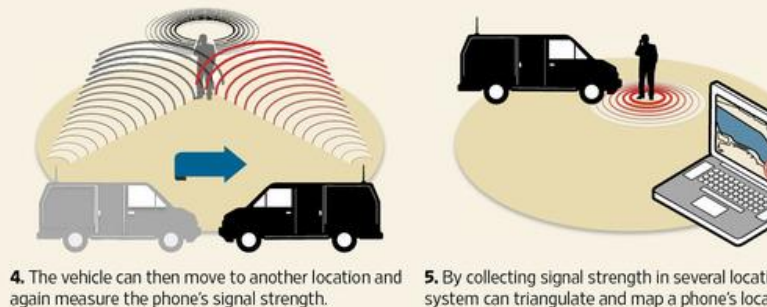
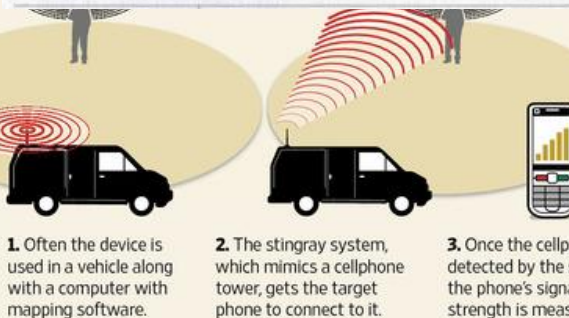
## 6. Cell Tracking

**USA TODAY**

### Police secretly track cellphones to solve routine crimes

**Your cell phone can be used to track you even when it is OFF!**

Law-enforcement officials are quietly using gadgets referred to generically as 'stingrays' to locate cellphones as part of investigative work.



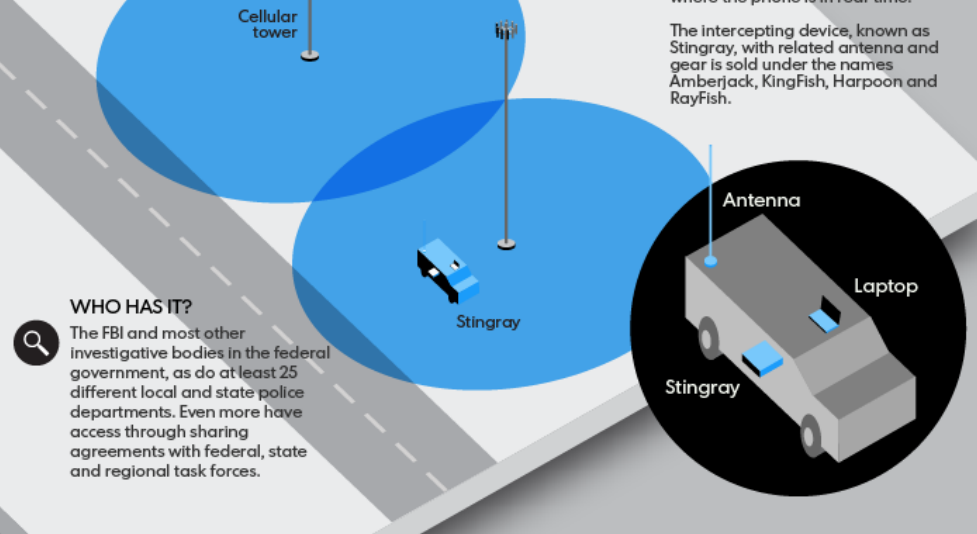
Source: WSJ research and government documents

### CELLULAR SURVEILLANCE!

The Feds know where you are right now!

#### HOW WORKS

A Stingray is a mobile device that masquerades as a cellphone tower. It's usually mounted in a police surveillance vehicle.



#### STINGRAY SYSTEM

Antennas on the police vehicle determine the distance and direction of the phone in relation to the Stingray and other cell towers, telling police where the phone is in real-time.

The intercepting device, known as Stingray, with related antenna and gear is sold under the names Amberjack, KingFish, Harpoon and RayFish.

#### WHO HAS IT?

The FBI and most other investigative bodies in the federal government, as do at least 25 different local and state police departments. Even more have access through sharing agreements with federal, state and regional task forces.



## 7. Tower Dumps

- 2703d Court Order that meets a relevant and material standard to all cell phone providers in a certain area that requires the provider to disclose all tower log records identifying all phones that contacted that cell tower during a specific time frame.
- Tower records are kept for a limited amount of time, so obtain records sooner rather than later.
- Multiple incidents, as well as a ***separation of time and distance*** between incidents, maximize effectiveness.
- Rural areas are nice, but not necessary.
- Takes time and money
- Not recommended for every investigation.



# Tower Dumps



CALLI NG_N BR	CALLE D_NB R	STAR T_DAT E	END_ DATE
(760) 828- 5992	(760) 298- 9393	Inboun d	3/1/13 1:53:1 2
(760) 298- 9393	(760) 828- 5992	Outbo und	3/1/13 2:00:1 0
(760) 828- 5992	(760) 298- 9393	Inboun d	3/1/13 2:04:5 2
(760) 298- 9393	(760) 622- 7700	Outbo und	3/1/13 2:13:1 6
(760) 298- 9393	(760) 588- 8463	Outbo und	3/1/13 2:39:1 6
(760) 298- 9393	(760) 588- 8463	Outbo und	3/1/13 2:39:3 5



# Tower Dumps



CALLI NG_N BR	CALLE D_NB R	M_R_#	STAR T_DAT E	END_ DATE
(760) 828- 5992	(760) 298- 9393	Inboun d	3/1/13 1:53:1 2	3/1/13 1:53:1 2
(760) 298- 9393	(760) 828- 5992	Outbo und	3/1/13 2:00:1 0	3/1/13 2:00:1 0
(760) 828- 5992	(760) 298- 9393	Inboun d	3/1/13 2:04:5 2	3/1/13 2:04:5 2
(760) 298- 9393	(760) 622- 7700	Outbo und	3/1/13 2:13:1 6	3/1/13 2:14:2 9
(760) 298- 9393	(760) 588- 8463	Outbo und	3/1/13 2:39:1 6	3/1/13 2:39:2 6
(760) 298- 9393	(760) 588- 8463	Outbo und	3/1/13 2:39:3 5	3/1/13 2:39:4 3

CALLIN G_NBR	CALLED NBR	M_R_#	START DATE	END_D ATE
(760) 828- 5992	(760) 298- 9393	Inboun d	3/1/13 1:53:12	3/1/13 1:53:12
(760) 298- 9393	(760) 828- 5992	Outbou nd	3/1/13 2:00:10	3/1/13 2:00:10
(760) 828- 5992	(760) 298- 9393	Inboun d	3/1/13 2:04:52	3/1/13 2:04:52
(760) 298- 9393	(760) 622- 7700	Outbou nd	3/1/13 2:13:16	3/1/13 2:14:29
(760) 298- 9393	(760) 588- 8463	Outbou nd	3/1/13 2:39:16	3/1/13 2:39:26
(760) 298- 9393	(760) 588- 8463	Outbou nd	3/1/13 2:39:35	3/1/13 2:39:43



# Tower Dumps



(760) 298-9393

Subscriber

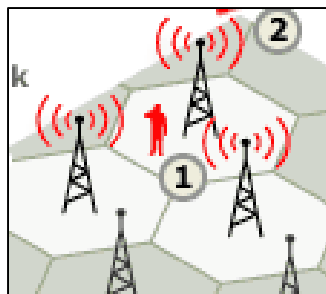
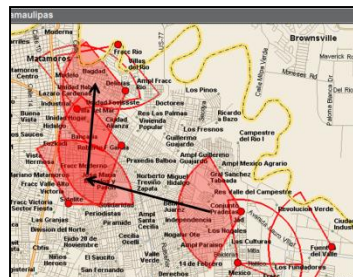
Call detail records

Historical locations

Real-time GPS



CALLI NG_N BR	CALLE D_NB R	M_R_#	STAR T_DAT E	END_ DATE
(760) 828- 5992	(760) 298- 9393	Inboun d	3/1/13 1:53:1 2	3/1/13 1:53:1 2
(760) 298- 9393	(760) 828- 5992	Outbo und	3/1/13 2:00:1 0	3/1/13 2:00:1 0
(760) 828- 5992	(760) 298- 9393	Inboun d	3/1/13 2:04:5 2	3/1/13 2:04:5 2
(760) 298- 9393	(760) 622- 7700	Outbo und	3/1/13 2:13:1 6	3/1/13 2:14:2 9
(760) 298- 9393	(760) 588- 8463	Outbo und	3/1/13 2:39:1 6	3/1/13 2:39:2 6
(760) 298- 9393	(760) 588- 8463	Outbo und	3/1/13 2:39:3 5	3/1/13 2:39:4 3

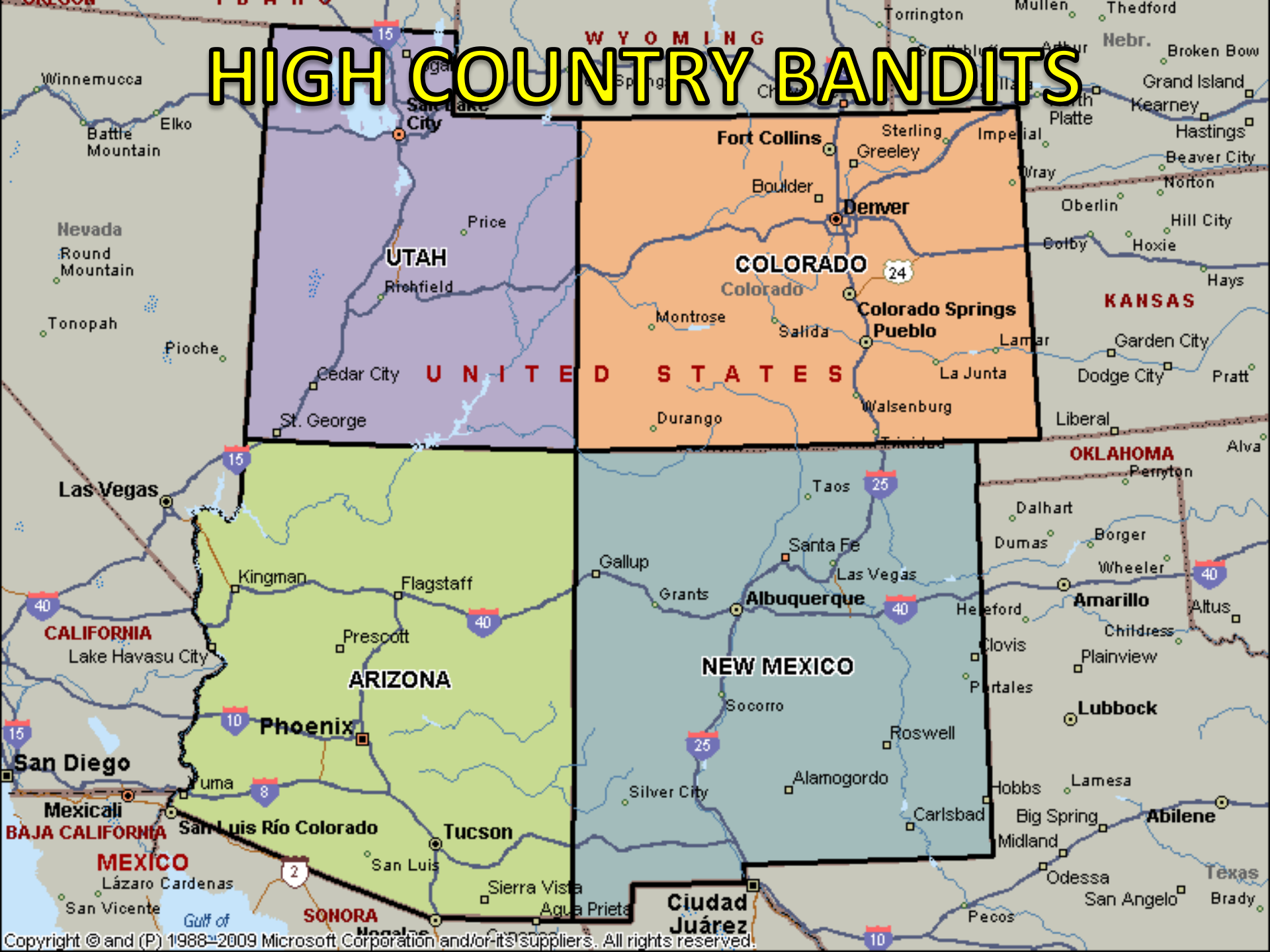


CALLIN G_NBR	CALLED NBR	M_R_#	START DATE	END_D ATE
(760) 828- 5992	(760) 298- 9393	Inboun d	3/1/13 1:53:12	3/1/13 1:53:12
(760) 298- 9393	(760) 828- 5992	Outbou nd	3/1/13 2:00:10	3/1/13 2:00:10
(760) 828- 5992	(760) 298- 9393	Inboun d	3/1/13 2:04:52	3/1/13 2:04:52
(760) 298- 9393	(760) 622- 7700	Outbou nd	3/1/13 2:13:16	3/1/13 2:14:29
(760) 298- 9393	(760) 888- 8463	Outbou nd	3/1/13 2:39:16	3/1/13 2:39:26
(760) 298- 9393	(760) 588- 8463	Outbou nd	3/1/13 2:39:35	3/1/13 2:39:43



# Cell Tower Dumps Case Example

# HIGH COUNTRY BANDITS



# Start of a Series

- 9/8/2009, Bank of the West, Heber, Arizona
- Suspect 1 enters bank brandishing semi-auto handgun, obtains money from several tellers
- Suspect 1 description: Male, black ski-mask, 5'7", unknown race and age
- Suspect 1 flees to back of ATV driven by Suspect 2 in full-face helmet. Both flee into mountainous area on ATV.
- As of 1/2010, we knew of 13 armed bank robberies covering 11 jurisdictions, 4 states and a geographic area of over 600 hundred miles.

# High Country Bandits M.O.

- One suspect in bank (WM, 5'8", thin, one glove) and one outside (WM, 6'0", larger build)
- Armed, take-over, closing time robberies hitting multiple tellers
- Suspect 1 has all victims ***"kiss the ground"***
- Most in rural areas supporting long distance ATV getaways
- Bank employee witness observed person matching Suspect description on a cell telephone before the Payson robbery





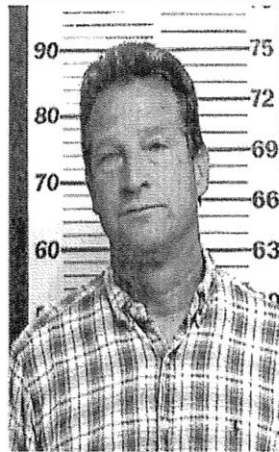
# Tower Dumps

- Two Uses:
  - Specific Crime: Determine phones used in the area
    - Preserve data in case a future suspect develops
    - Narrow suspect pool based on knowledge (outgoing call only, 3 minute conversation, not in area after crime, etc.)
  - Multiple Crimes: Different locations and times
    - *Compare data received for a common number*

# Suspect?

- Over 180,000 numbers obtained
- One Verizon number, 928-205-8558, using cell towers at 3 of 4 robbery locations
- Number used by Ron Capito, a WM, 6'2", 230 lbs

SHOW LOW POLICE DEPARTMENT							Page 1
PERSON RECORD							03/05/2010
CAPITO, RONALD MICHAEL							
Address 7013 BOULDER CREEK RD, SHOW LOW, AZ 85901			Mailing Address				
ID 53145	Phone 928-532-5436	DOB [REDACTED]	Age 52	Sex M	Height 6'	Weight 200	
Race WHITE			Hair BROWN		Eyes GREEN		
Drivers License B [REDACTED]		SSN [REDACTED]	St ID [REDACTED]	Vehicle License [REDACTED]		FBI #	
Business Name		Address		City & State Linden, AZ 85901			
Business Phone 928-532-5436		Gang Affiliation		Arrest ID 10640			
Next of Kin/Parent/Guardian [REDACTED]		Address [REDACTED]			Phone 532-5436		
Occupation SELF EMPLOYED CONTRACTOR						Undocumented Alien NO	
Complexion CLEAR		Build MUSCULAR		Hairstyle SHORT		Facial Hair NONE	Speech CLEAR
						Glasses NO	



# If Capito Is Suspect 2, Who Is Suspect 1?

- Analysis of Capito's phone showed he was contacting a phone used by Joel Glore, at 2 of the 4 robberies



photo image date 11/27/2007



# Flood Gates Opened

## ARIZONA GAME AND FISH DEPARTMENT

PINETOP REGION  
2878 E. WHITE MOUNTAIN BLVD.  
PINETOP, AZ 85935  
PHONE: (928) 367-4281  
FAX: (928) 367-1258

### STATEMENT OF FACT

SUSPECT NAME: CAPITO, RONALD M.

CITATION# 232173

On September 4, 2009 Ronald M. CAPITO was issued a citation by AZ Game and Fish Officer R. BIRKELAND for "Riding Double on an ATV or against manufacturer's specifications (ATV designed for one person)" – ARS 28-892. CAPITO was the operator on an ATV manufactured for one rider only. The passenger was identified as Joel J. Glore (9-27-1958). This incident took place in Navajo County along State Highway 260 in Heber, AZ.

On September 4, 2009 Officer BIRKELAND was traveling east on State Highway 260 on the west end of Heber. Officer BIRKELAND noticed an all terrain vehicle (ATV) traveling at a high rate of speed, also going east on State Highway 260. The ATV was going downhill at approximately 40 miles per hour, carrying a passenger, and swerving. There was a lot of holiday weekend traffic, some of which was backed up behind this ATV. Due to this being a public safety issue, Officer BIRKELAND initiated a



Only 4 days before the Heber robbery.

On September 4, 2009 Ronald M. CAPITO was issued a citation by AZ Game and Fish Officer R. BIRKELAND for "Riding Double on an ATV or against manufacturer's specifications (ATV designed for one person)" – ARS 28-892. CAPITO was the operator on an ATV manufactured for one rider only. The passenger was identified as Joel J. Glore (9-27-1958). This incident took place in Navajo County along State Highway 260 in Heber, AZ.

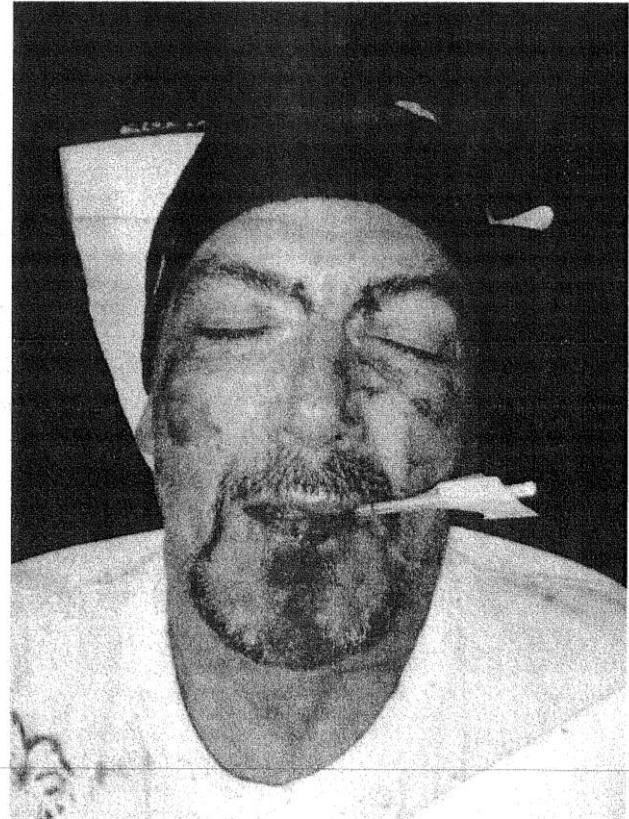


# Flood Gates Opened

As they were returning from the Park City robbery, Capito assaults Glore. Cash and handguns were found in their car.



RONALD MICHAEL CAPITO  
02/25/58  
6'00"  
200 lbs  
BROWN  
HAZEL  
MEDIUM COMPLEXION  
POB SCOTTSDALE, AZ



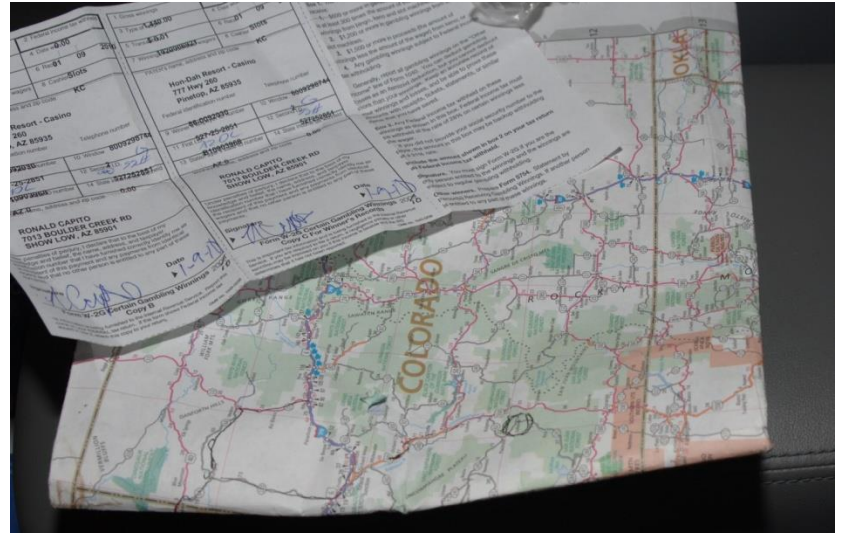
incident# S10-0189, Assault

# Capito Residence Search

- Out in the open are the cars, ATV he actually owns, and other signs of a successful person
- Hidden are the indicators of the double life he is leading



# Capito Residence Search



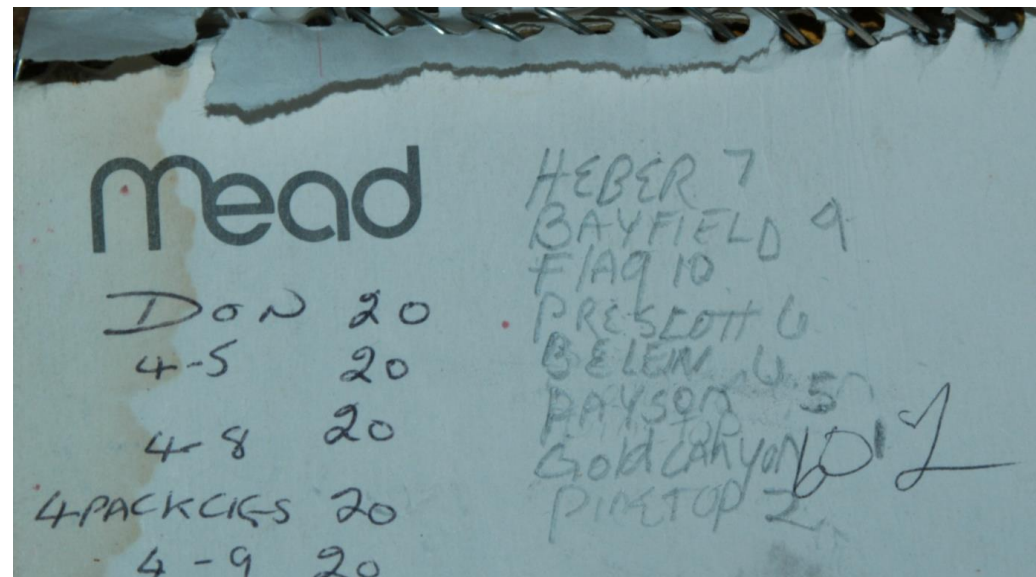
# Glore Residence Search



- Nothing is “hidden” in this place, all in the open.



# Glore Residence Search





## 8. Drop Phones

\* Better than nothing!\*

HO-EJ Ver: 1.00

ST# 3896 OP# 00000170 TE# 67 TR# 06235

TE# 67 OP# 00000170 TR# 06235

DT 062812 TM 165153

PHONE CARD ACTIVATED#

POP# 56932254640493398933524

VZW SAM U365 063575349784S 14.88 AD

TE# 67 OP# 00000170 TR# 06235

DT 062812 TM 165204

PHONE CARD ACTIVATED#

POP# 36928984640493398933524

VZW SAM U365 063575349784S 14.88 AD

SUBTOTAL 29.76

SALES TAX 1 2.71

TOTAL 32.47

CASH TEND 35.00

CHANGE DUE 2.53

\*\*\*SURVEY OFFERED\*\*\*

TC# 9233 0361 0777 1845 8316

06/28/12 16:52:28



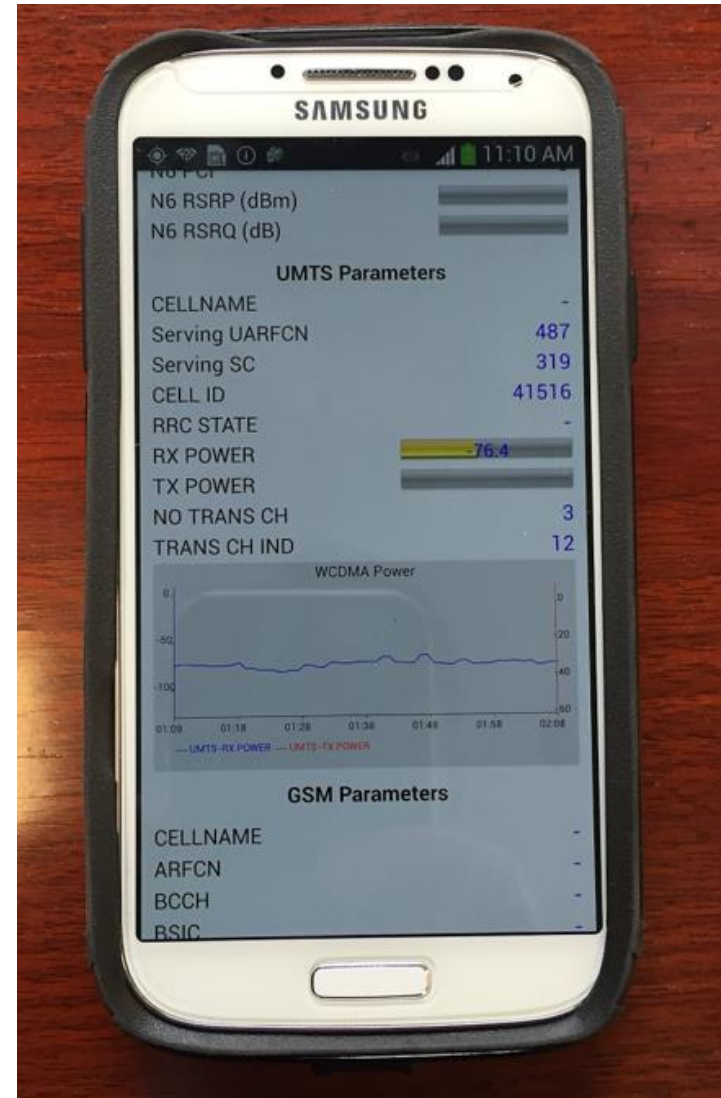


## 9. SMS Content

- Provider Records vs. Records on Device
  - Provider Records
    - Few providers save text content
    - Limited time
    - Preservation Letter
    - Search warrant or exigency [18 U.S.C. § 2702(b)(8)]
  - Records on Device
    - Cellebrite or other forensic platforms
      - Physical vs. Logical
    - Often shows apps/wi-fi text messages that do not show on provider records (ie iMessages)
- CONTENT!



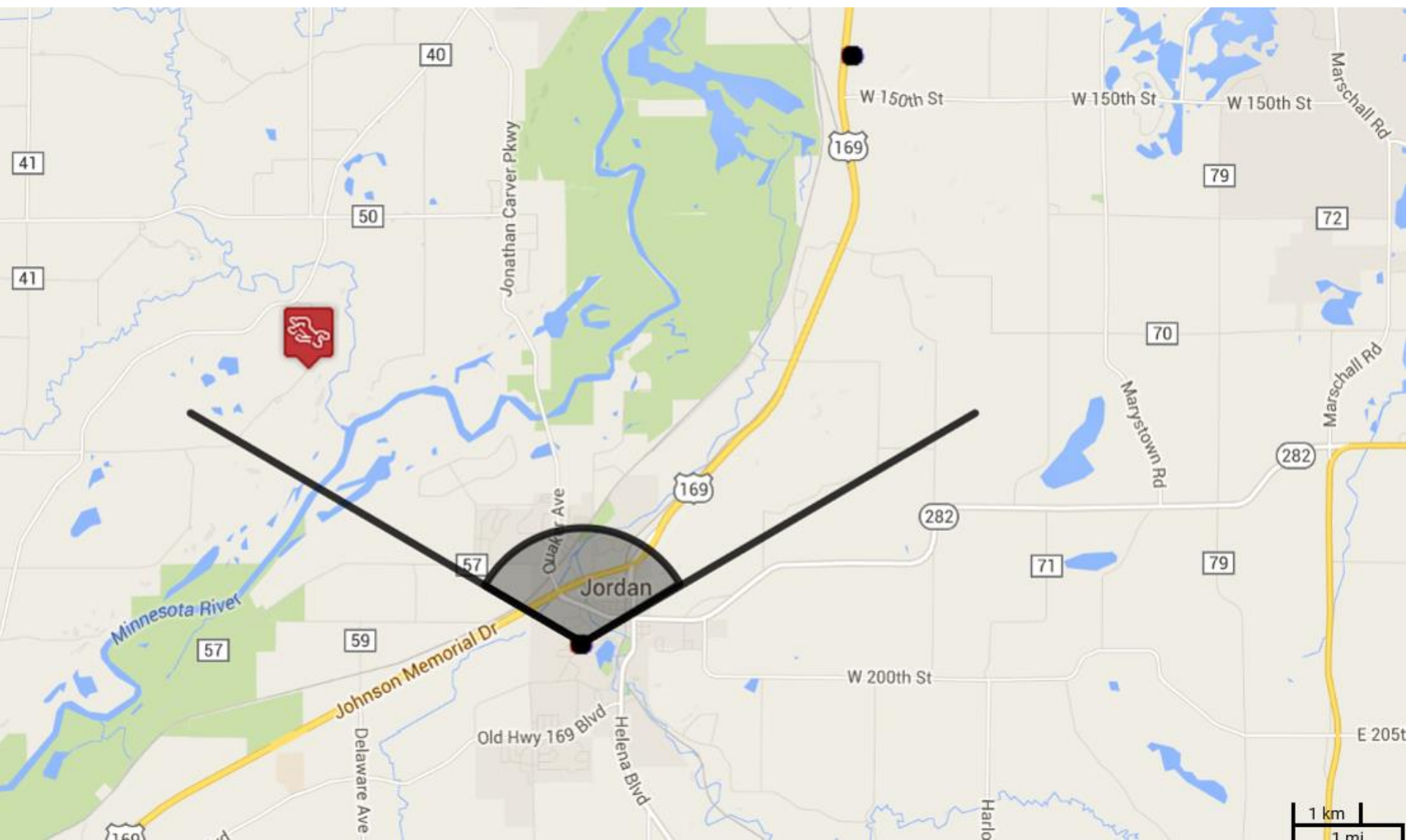
## 10. Network Survey Drive Testing





# Network Survey Drive Test

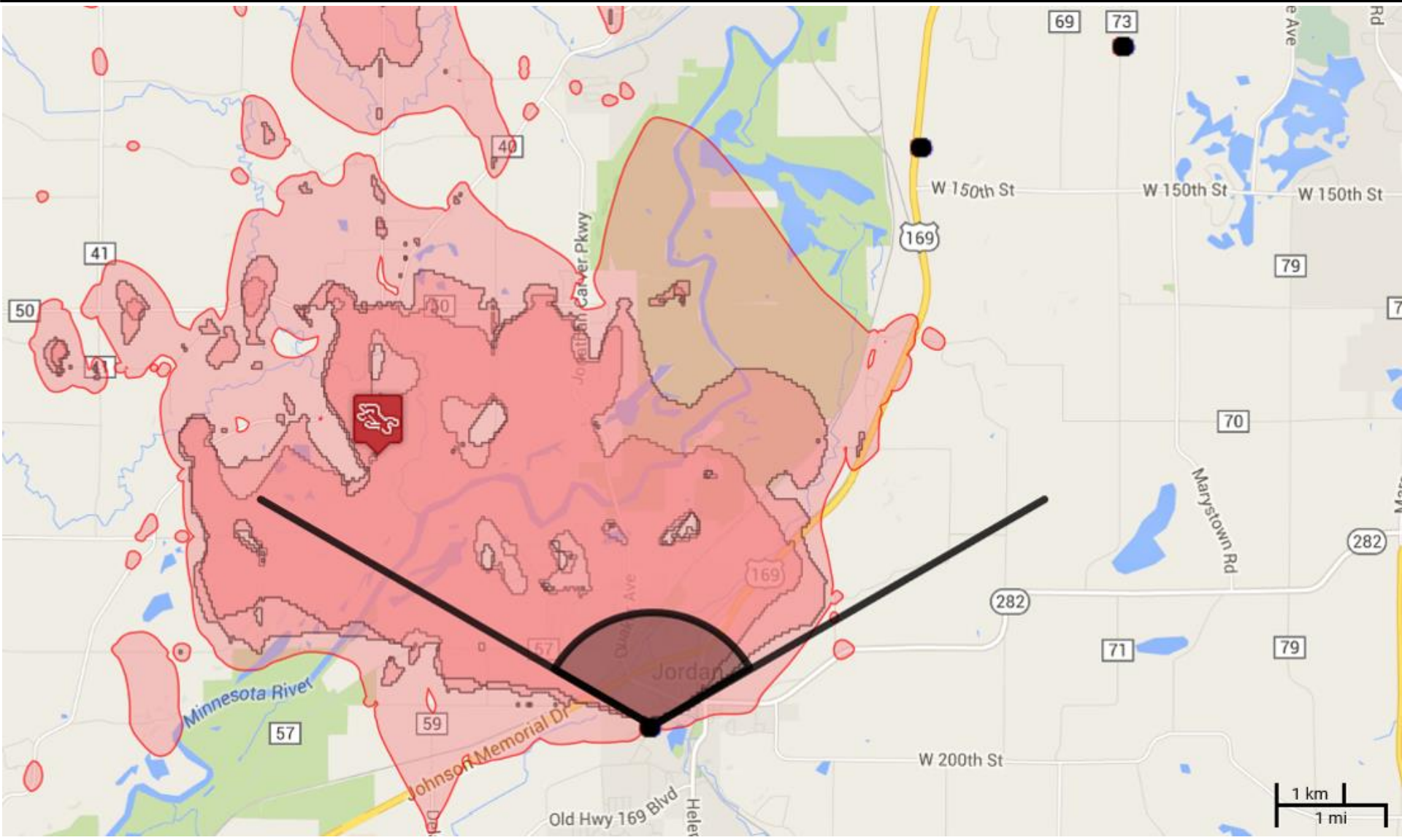
(BEFORE - Tower and Sector Usage)





# Network Survey Drive Test

(AFTER - Actual RF footprint of sector)



# What CAST does



- Review Case Summary
- Review and analyze CDRs
- Utilize CAST specific tools
  - Telephone Analysis Package
  - ESPA Cellular Analysis
  - Tower Dump Utility
  - Round Trip Delay Measurement
- Plot a Preliminary Analysis

If the CAST Agent and Case Agent find it necessary, the CAST Agent will then perform the following functions.

- Network Survey Drive Testing
- Post Processing of drive test data
- Create a mapping product (Map Point, Google Earth)
- Prepare a written report and presentation for court

# What CAST will do for YOU (as a prosecutor)

- Prepare a draft analysis historical cell site analysis report
- Have the report peer reviewed
- Prepare a final written report and presentation for court
- Provide a Curriculum Vitae (CV)
- Provide a testimony introduction script
- Testify as an expert re historical cell site analysis
- Consult re defense expert report/testimony





# Some Things to Consider

- Placing the cell phone in the defendant's hands is more than 50% of your battle
- Although cell phone evidence isn't always incriminating, should you put it on anyway to show due diligence and cover the CSI factor?
- Obtain records certification and get CDRs stipulated to where possible
- Custodians of Record should NOT be testifying about cellular technology, OBJECT if this starts to happen during cross



**SA Geoffrey Young**  
**Phoenix Field Office**  
**602-725-6670 – cell**  
**GRYOUNG@FBI.GOV**

**CAST@IC.FBI.GOV**